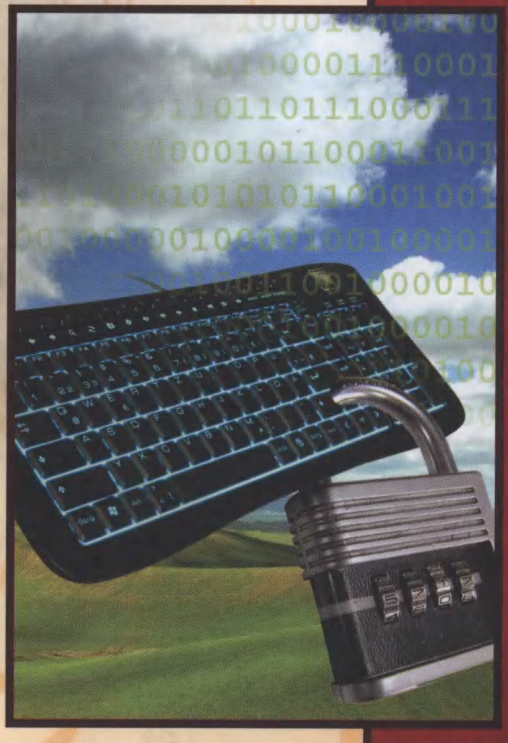
ВЫСШЕЕ ОБРАЗОВАНИЕ

КОМПЛЕКСНАЯ ЗАЩИТА ИНФОРМАЦИИ В КОРПОРАТИВНЫХ СИСТЕМАХ



В.Ф. Шаньгин

ИЗДАТЕЛЬСКИЙ ДОМ ФОРУМ

В. Ф. Шаньгин

КОМПЛЕКСНАЯ ЗАЩИТА ИНФОРМАЦИИ В КОРПОРАТИВНЫХ СИСТЕМАХ

Допущено Учебно-методическим объединением вузов по университетскому политехническому образованию в качестве учебного пособия для студентов высших учебных заведений, обучающихся по направлению 230100 «Информатика и вычислительная техника»

Москва
ИД «ФОРУМ» — ИНФРА-М
2010

УДК 002.56(075.8)
ББК 32.973я73
Ш20

Рецензенты:
доктор технических наук, профессор, зав. кафедрой «Информатика и программное обеспечение вычислительных систем» Московского государственного института электронной техники (Технического университета) *Л. Г. Гагарина*;
кандидат технических наук, доцент кафедры «Информационные технологии» филиала Санкт-Петербургского гуманитарного университета профсоюзов *А. А. Петров*

Шаньгин В. Ф.
Ш20 Комплексная защита информации в корпоративных системах : учеб. пособие / В. Ф. Шаньгин. — М. : ИД «ФОРУМ» : ИНФРА-М, 2010. — 592 с. : ил. — (Высшее образование).

ISBN 978-5-8199-0411-4 (ИД «ФОРУМ»)
ISBN 978-5-16-003746-2 (ИНФРА-М)

Книга посвящена методам и средствам комплексной защиты информации в корпоративных системах. Формулируются основные понятия защиты информации, анализируются угрозы информационной безопасности в корпоративных системах. Обсуждаются базовые понятия и принципы политики безопасности. Описываются криптографические методы и алгоритмы защиты корпоративной информации. Обсуждаются методы и средства идентификации, аутентификации и управления доступом в корпоративных системах. Анализируются методы защиты электронного документооборота. Обосновывается комплексный подход к обеспечению информационной безопасности корпоративных систем. Рассматриваются средства обеспечения безопасности операционных систем UNIX и Windows Vista. Обсуждаются методы и средства формирования виртуальных защищенных каналов и сетей. Описываются функции межсетевых экранов. Рассматриваются методы предотвращения вторжений в корпоративные информационные системы. Обсуждаются методы и средства защиты от вредоносных программ. Рассматриваются методы управления средствами обеспечения информационной безопасности. Анализируются международные и отечественные стандарты информационной безопасности.

Для студентов высших учебных заведений, обучающихся по направлению «Информатика и вычислительная техника», а также может быть полезна студентам, аспирантам и преподавателям вузов соответствующих специальностей.

УДК 002.56(075.8)
ББК 32.973я73

ISBN 978-5-8199-0411-4 (ИД «ФОРУМ»)
ISBN 978-5-16-003746-2 (ИНФРА-М)

Предисловие

Быстрое развитие информационных технологий и глобальной сети Интернет привело к формированию информационной среды, оказывающей влияние на все сферы человеческой деятельности. Корпоративные информационные системы (КИС) становятся сегодня важнейшим средством производства современной компании, они позволяют преобразовать традиционные формы бизнеса в электронный бизнес. Электронный бизнес использует глобальную сеть Интернет и современные информационные технологии для повышения эффективности всех сторон деятельности компаний, включая производство, маркетинг, продажи, платежи, финансовый анализ, поиск сотрудников, поддержку клиентов и партнерских отношений.

Важным условием существования электронного бизнеса является *информационная безопасность*, под которой понимается защищенность корпоративной информации и поддерживающей инфраструктуры от случайных и преднамеренных воздействий, которые могут нанести ущерб владельцам или пользователям информации. Ущерб от нарушения информационной безопасности может привести к крупным финансовым потерям и даже к полному закрытию компании. Поэтому проблемы обеспечения информационной безопасности привлекают внимание как специалистов в области компьютерных систем и сетей, так и многочисленных пользователей, включая компании, работающие в сфере электронного бизнеса. Задача обеспечения безопасности корпоративных информационных систем решается путем построения комплексной системы информационной безопасности.

Без знания и квалифицированного применения современных информационных технологий, стандартов, протоколов и средств защиты информации невозможно достигнуть требуемого уровня информационной безопасности компьютерных систем и сетей.

Предлагаемое вниманию читателя учебное пособие посвящено систематическому изложению и анализу современных методов, средств и технологий комплексной защиты информации в корпоративных системах.

Содержание книги разбито на четыре логически связанные части:

- часть I «Проблемы безопасности корпоративной информации»;
- часть II «Технологии защиты корпоративных данных»;
- часть III «Комплексная защита корпоративных информационных систем»;
- часть IV «Управление информационной безопасностью».

Каждая из этих частей объединяет несколько глав, связанных общей темой. Каждая глава завершается набором вопросов для самокон-

троля. Книга содержит также предисловие, введение, список сокращений и список литературы.

Часть I «Проблемы безопасности корпоративной информации» включает следующие главы:

- глава 1 «Основные понятия информационной безопасности»;
- глава 2 «Проблемы информационной безопасности сетей»;
- глава 3 «Политика безопасности».

В главе 1 формулируются основные понятия и определения информационной безопасности и анализируются угрозы информационной безопасности в корпоративных информационных системах.

Глава 2 сначала вводит в сетевой информационный обмен и коммуникационные протоколы ISO/OSI и TCP/IP. Затем в этой главе анализируются угрозы и уязвимости проводных и беспроводных сетей, формулируются способы обеспечения информационной безопасности и возможные пути решения проблем защиты информации в сетях.

В главе 3 определяются базовые понятия политики безопасности и описываются основные виды политик и процедур безопасности в корпоративных информационных системах.

Часть II «Технологии защиты корпоративных данных» включает следующие главы:

- глава 4 «Криптографическая защита информации»;
- глава 5 «Идентификация, аутентификация и управление доступом»;
- глава 6 «Защита электронного документооборота».

В главе 4 описываются такие криптографические методы защиты корпоративной информации, как симметричные и асимметричные криптосистемы шифрования, комбинированные криптосистемы, электронная цифровая подпись, функции хэширования и управление криптоключами. Подробно описывается инфраструктура управления открытыми ключами PKI (Public Key Infrastructure).

Глава 5 посвящена рассмотрению идентификации, аутентификации и авторизации пользователя. Описываются методы аутентификации, использующие многоразовые и одноразовые пароли, методы строгой аутентификации и биометрической аутентификации пользователей, управление доступом по схеме однократного входа Single Sign-On.

В главе 6 рассматриваются методы и средства защиты электронного документооборота. Формулируется концепция и особенности защиты электронного документооборота. Анализируются методы и средства защиты баз данных. Подробно описывается защита электронного почтового документооборота. Рассмотрена реализация отечественной системы защищенного электронного документооборота и управления взаимодействием DIRECTUM.

Часть III «Комплексная защита корпоративных информационных систем» объединяет следующие главы:

- глава 7 «Принципы комплексной защиты корпоративной информации»;
- глава 8 «Безопасность операционных систем»;

- глава 9 «Протоколы защищенных каналов»;
- глава 10 «Межсетевое экранирование»;
- глава 11 «Виртуальные защищенные сети VPN»;
- глава 12 «Защита удаленного доступа»;
- глава 13 «Обнаружение и предотвращение вторжений»;
- глава 14 «Защита от вредоносных программ и спама».

Глава 7 посвящена рассмотрению принципов комплексной защиты информации в корпоративных информационных системах. Анализируются особенности архитектуры КИС и структура системы защиты информации в КИС. Формулируется стратегия комплексного обеспечения информационной безопасности, и описываются основные подсистемы информационной безопасности КИС.

В главе 8 анализируются угрозы безопасности в операционных системах (ОС), вводится понятие защищенной ОС, описываются архитектура и основные функции подсистемы защиты ОС. Рассматриваются средства обеспечения безопасности операционных систем UNIX и Windows Vista.

В главе 9 обсуждаются проблемы построения защищенных виртуальных каналов на канальном, сетевом и сеансовом уровнях эталонной модели взаимодействия открытых систем OSI. Рассматриваются особенности применения протоколов на канальном уровне PPTP, L2F и L2TP. Описываются архитектура стека протоколов IPSec, протокол аутентификации AH, протокол формирования защищенного пакета ESP, протокол управления криптоключами IKE. Приводятся сведения об алгоритмах аутентификации и шифрования, применяемых в стеке протоколов IPSec. Описывается применение протоколов SSL и SOCKS для построения защищенных каналов на сеансовом уровне. Рассматривается защита беспроводных сетей.

В главе 10 рассматриваются функции межсетевых экранов. Описываются схемы сетевой защиты на базе межсетевых экранов. Рассматривается применение персональных и распределенных сетевых экранов.

Глава 11 представляет собой введение в защищенные виртуальные сети VPN (Virtual Private Network). Поясняется главное свойство сети VPN — туннелирование. Анализируются варианты построения виртуальных защищенных каналов. Рассматриваются варианты архитектуры сетей VPN, и приводятся основные виды технической реализации VPN.

В главе 12 рассматривается организация защищенного удаленного доступа, анализируются протоколы аутентификации и системы централизованного контроля удаленного доступа. Особое внимание уделяется протоколу аутентификации Kerberos.

Глава 13 посвящена проблемам обнаружения и предотвращения вторжений. Рассматриваются методы обнаружения и предотвращения вторжений в корпоративные информационные системы, а также защита от распределенных атак.

В главе 14 описываются средства защиты от вредоносных программ и спама. Приводится классификация вредоносных программ. Рассматриваются сигнатурный анализ и проактивные методы обнаружения ви-

русов и других вредоносных программ. Описывается защита корпоративной системы от вредоносных программ.

Часть IV «Управление информационной безопасностью» объединяет следующие главы:

- глава 15 «Управление средствами обеспечения информационной безопасности»;
- глава 16 «Стандарты информационной безопасности».

В главе 15 рассматриваются методы управления средствами защиты корпоративной информации. Сформулированы задачи управления системой информационной безопасности масштаба предприятия. Анализируются варианты архитектуры управления средствами безопасности. Особое внимание уделяется перспективной архитектуре централизованного управления безопасностью на базе глобальной и локальной политик безопасности. Приводится обзор современных систем управления информационной безопасностью.

Глава 16 посвящена описанию стандартов информационной безопасности. Рассматриваются основные международные стандарты информационной безопасности. Даны краткие описания популярных стандартов информационной безопасности для Интернета. Описываются отечественные стандарты безопасности информационных технологий.

Материал книги базируется только на открытых публикациях в Интернете, отечественной и зарубежной печати. В основу книги положены материалы лекций, читаемых автором в Московском государственном институте электронной техники.

Автор заранее благодарен читателям, которые пришлют ему свои замечания и пожелания по адресу shanico@mail.ru.

Список сокращений

3-DES (Triple Data Encryption Standard) — алгоритм тройного шифрования, разновидность алгоритма DES.

ACK (Acknowledgement) — подтверждение.

AES (Advanced Encryption Standard) — американский стандарт шифрования данных.

AH (Authentication Header) — аутентифицирующий заголовок в IPSec.

AP (Access Point) — точка доступа — коммуникационный узел для пользователей или беспроводное устройство.

AS (Authentication Server) — сервер аутентификации.

ASA (Adaptive Security Algorithm) — алгоритм адаптивной безопасности.

B2B (Business-to-Business) — схема бизнес—бизнес: модель ведения бизнеса в Интернете на уровне компаний.

B2C (Business-to-Consumer) — схема бизнес—потребитель: розничная продажа товаров и услуг частным лицам через Интернет.

CA (Certification Authority) — центр сертификации.

CEK (Content Encryption Key) — ключ шифрования данных.

CHAP (Challenge-Handshake Authentication Protocol) — протокол аутентификации на основе процедуры запрос—отклик.

CRL (Certificate Revocation List) — список аннулированных сертификатов.

DDoS (Distributed Denial of Service) — распределенная атака отказа в обслуживании.

DES (Data Encryption Standard) — бывший стандарт шифрования данных США.

DH (Diffie — Hellman) — Диффи — Хеллман.

DHCP (Dynamic Host Configuration Protocol) — протокол динамической конфигурации хостов.

DMZ (Demilitarized Zone) — демилитаризованная зона, безопасная зона сети.

DNS (Domain Name Server) — служба имен доменов.

DOI (Domain of Interpretation) — область интерпретации.

DoS (Denial of Service) — атака отказа в обслуживании.

DSSS (Direct Sequence Spread Spectrum) — распределенный спектр с прямой последовательностью.

EAP (Extensible Authentification Protocol) — расширяемый протокол аутентификации.

ECC (Elliptic Curve Cryptography) — криптография эллиптических кривых.

EE (End Entity) — конечный пользователь.

EEPROM (Electrically Erasable Programmable Read-only Memory) — электрически программируемая память только для чтения данных.

ESP (Encapsulated Security Payload) — встроенная полезная нагрузка безопасности для IPSec.

FHSS (Frequency Hopping Spread Spectrum) — распределенный спектр со скачками по частотам.

FTP (File Transfer Protocol) — протокол передачи файлов.

GPS (Global Positioning System) — система глобального позиционирования.

GSP (Global Security Policy) — глобальная политика безопасности для всей VPN.

HMAC (Hashing for Message Authentication) — аутентификация сообщений с хэшированием по ключам.

HTTP (HyperText Transfer Protocol) — протокол передачи гипертекстовых файлов.

ICMP (Internet Control Message Protocol) — протокол управляющих сообщений в сети Интернет.

ICV (Integrity Check Value) — значение проверки целостности.

IDS (Intrusion Detection System) — система определения вторжений.

IEEE (Institute of Electrical and Electronics Engineers) — Институт инженеров по электротехнике и радиоэлектронике.

IEEE 802.11 — группа разработки стандартов в IEEE, цель которой — выпуск стандартов беспроводных локальных сетей LAN.

IKE (Internet Key Exchange) — протокол обмена ключами в Интернете.

IP (Internet Protocol) — интернет-протокол межсетевого обмена данными.

IPS (Intrusion Prevention System) — система предотвращения вторжений.

IPSec (Internet Security Protocol) — интернет-протокол безопасного межсетевого обмена.

IPv4 (Internet Protocol, version 4) — интернет-протокол межсетевого обмена, версия 4.

IPv6 (Internet Protocol, version 6) — интернет-протокол межсетевого обмена, версия 6.

ISAKMP (Internet Security Association and Key Management Protocol) — протокол безопасных ассоциаций и управления ключами Интернета.

ISDN (Integrated Services Digital Network) — цифровые сети с интегральными услугами.

ISO (International Standards Organization) — Международная организация по стандартизации.

ISP (Internet Service Provider) — поставщик услуг Интернета.

IT (Information Technology) — информационная технология.

KEK (Key-Encryption Key) — ключ для шифрования ключей.

KS (Kerberos Server) — сервер системы Kerberos.

L2F (Layer-2 Forwarding) — протокол передачи данных второго (канального) уровня.

L2TP (Layer-2 Tunneling Protocol) — протокол туннелирования данных второго (канального) уровня.

LAC (L2TP Access Concentrator) — концентратор доступа L2TP.

LAN (Local Access Network) — локальная сеть.

LCP (Link Control Protocol) — протокол управления соединением.

LDAP (Lightweight Directory Access Protocol) — облегченный протокол доступа к каталогам.

LNS (L2TP Network Server) — сетевой сервер L2TP.

LSP (Local Security Policy) — локальная политика безопасности (для клиента).

MAC (Media Access Control) — управление доступом к среде.

MAC (Message Authentication Code) — код аутентификации сообщения.

MAN (Metropolitan Area Network) — городская сеть.

MD (Message Digest) — дайджест сообщения.

MIB (Management Information Base) — стандарт базы данных для управления сетью.

MIF (Management Information File/Format) — формат для файлов управляющей информации.

MITM (Man In The Middle) — сетевая атака «человек-в-середине».

MTU (Maximum Transmission Unit) — максимальный размер передаваемого блока.

NAK (Negative Acknowledgement) — подтверждение отказа.

NAS (Network Access Server) — сервер доступа к сети.

NAT (Network Address Translation) — трансляция сетевых адресов.

NCP (Network Control Protocol) — протокол управления сетью.

NIDS (Network-based Intrusion Detection System) — система обнаружения вторжений в сеть.

NNM (Network Node Manager) — система сетевого управления.

OCSP (Online Certificate Status Protocol) — протокол статуса текущего сертификата.

OSI (Open Systems Interconnection) — взаимодействие открытых систем.

OTK (One-Time Key) — одноразовый ключ.

OTP (One-Time Password) — одноразовый пароль.

PAP (Password Authentication Protocol) — протокол аутентификации по паролю.

PDA (Personal Digital Assistant) — карманный персональный компьютер, КПК.

PGP (Pretty Good Privacy) — достаточно хорошая секретность.

PKD (Public Key Directory) — каталог открытых ключей.

PKI (Public Key Infrastructure) — инфраструктура управления открытыми ключами.

PPP (Point-to-Point Protocol) — протокол двухточечного соединения.

PPTP (Point-to-Point Tunneling Protocol) — протокол туннелирования для двухточечного соединения.

QOS (Quality of Service) — качество предоставляемых услуг.

RADIUS (Remote Authentication Dial-In User Service) — система удаленной аутентификации пользователей по коммутируемым линиям.

RAS (Remote Access Service) — служба удаленного доступа.

RC4 (Rivest Cipher 4) — потоковый шифр, разработанный Роном Райвестом и используемый в базовом стандарте IEEE 802.11.

RFC (Request For Comments) — запрос комментариев.

RFID (Radio Frequency Identifier) — радиочастотный идентификатор.

RPC (Remote Procedure Call) — удаленный вызов процедуры.

RSA (Rivest—Shamir—Adleman) — Райвест—Шамир—Эйдельман.

SA (Security Associations) — безопасные ассоциации.

SAD (Security Associations Database) — база данных безопасных ассоциаций.

SET (Secure Electronic Transaction) — стандарт защищенных электронных транзакций.

SHA-1 (Secure Hash Algorithm) — алгоритм защищенного хэширования, используемый в США.

SKIP (Simple Key management for Internet Protocols) — простое управление ключами для интернет-протоколов.

SMTP (Simple Mail Transfer Protocol) — простой протокол электронной почты.

SNMP (Simple Network Management Protocol) — простой протокол сетевого управления.

SOHO (Small Office/Home Office) — решения для малых и домашних офисов.

SPD (Security Policy Database) — база данных правил безопасности.

SPI (Security Parameter Index) — индекс параметров защиты.

SQL (Structured Query Language) — структурированный язык запросов.

SSH (Secure Shell) — безопасный уровень. Протокол и программа SSH обеспечивают надежные шифрование и аутентификацию.

SSL (Secure Sockets Layer) — уровень безопасных соединений. Протокол для установки шифрованных соединений между интернет-сервером и интернет-браузером.

TACACS (Terminal Access Controller Access Control System) — протокол централизованного контроля удаленного доступа.

TCP (Transport Control Protocol) — протокол управления передачей.

TGS (Ticket Granting Server) — сервер выдачи разрешений.

TLS (Transport Layer Security) — защита транспортного уровня.

UDP (User Data Protocol) — протокол передачи данных пользователя.

URL (Uniform Resource Locator) — унифицированный указатель ресурса.

VPN (Virtual Private Network) — защищенная виртуальная сеть.

WAN (Wide Area Network) — сеть, развернутая на большой территории.

WWW (World Wide Web) — служба гипертекстовой информации Интернета.

Введение

Деятельность современной компании невозможна без использования информационных технологий. Эффективное применение информационных технологий является общепризнанным фактором роста конкурентоспособности компании. Многие предприятия в мире переходят к использованию широких возможностей Интернета и электронного бизнеса. *Корпоративные информационные системы* (КИС) становятся сегодня одним из главных инструментов управления бизнесом и фактически важнейшим средством производства современной компании. В таких условиях одним из наиболее ценных ресурсов организации является *корпоративная информация*.

Все больше корпоративных систем, приложений и данных становятся доступными из Глобальной сети, вследствие чего компании сталкиваются с возрастающим числом различных угроз для своей информационной инфраструктуры — несанкционированный доступ, вирусная опасность, атаки типа «отказ в обслуживании» и другие виды вторжений, мишенью для которых становятся приложения, компьютерные сети и инфраструктура КИС.

Поэтому применение информационных технологий немыслимо без повышенного внимания к вопросам информационной безопасности. Одной из самых актуальных задач, которая стоит сегодня перед разработчиками и поставщиками информационных технологий, является решение проблем информационной безопасности, связанных с широким распространением Интернета, интранета и экстранета.

Реализация решений для электронного бизнеса должна обеспечивать хорошую защиту, конфиденциальность транзакций, предоставлять защиту целостности выполнения деловых операций и данных заказчиков, а также гарантировать постоянный доступ к данным. Информация должна быть доступна только тем, кому она предназначена, и скрыта от сторонних наблюдателей. Несанкционированное использование информационного ресурса, его временная недоступность или разрушение могут нанести компании значительный материальный ущерб. Надежная защита информационных ресурсов повышает эффективность всего процесса информатизации, обеспечивая безопасность дорогостоящей деловой информации, циркулирующей в локальных и глобальной информационных средах.

Использование Интернета в качестве глобальной публичной сети означает для средств безопасности предприятия не только резкое увеличение количества внешних пользователей и разнообразие типов коммуникационных связей, но и сосуществование с новыми сетевыми и

информационными технологиями. Поэтому информационные ресурсы и средства осуществления электронных сетевых транзакций (серверы, маршрутизаторы, серверы удаленного доступа, каналы связи, операционные системы, базы данных и приложения) нужно защищать особенно надежно и качественно.

Следует заметить, что средства взлома компьютерных сетей и хищения информации развиваются так же быстро, как и все высокотехнологичные компьютерные отрасли. В этих условиях обеспечение информационной безопасности КИС является приоритетной задачей, поскольку от сохранения конфиденциальности, целостности и доступности корпоративных информационных ресурсов во многом зависит эффективность работы КИС.

Задача обеспечения информационной безопасности КИС традиционно решается построением *системы информационной безопасности* (СИБ), определяющим требованием к которой является сохранение вложенных в построение КИС инвестиций. Иначе говоря, СИБ должна функционировать абсолютно прозрачно для уже существующих в КИС приложений и быть полностью совместимой с используемыми в КИС сетевыми технологиями.

Создаваемая система информационной безопасности предприятия должна учитывать появление новых технологий и сервисов, а также удовлетворять общим требованиям, предъявляемым сегодня к корпоративной информационной системе:

- *применение открытых стандартов*;
- *использование интегрированных решений*;
- *обеспечение масштабирования в широких пределах*.

Переход на открытые стандарты составляет одну из главных тенденций развития современных средств информационной безопасности. Такие стандарты, как IPSec и PKI, обеспечивают защищенность внешних коммуникаций предприятий и совместимость с соответствующими продуктами предприятий-партнеров или удаленных клиентов. Цифровые сертификаты X.509 также являются на сегодня стандартной основой для аутентификации пользователей и устройств. Перспективные средства защиты, безусловно, должны поддерживать эти стандарты сегодня.

Под *интегрированными решениями* понимаются как интеграция средств защиты с остальными элементами сети (операционными системами, маршрутизаторами, службами каталогов, серверами QoS-политики и т. п.), так и интеграция различных технологий безопасности между собой для обеспечения *комплексной защиты* информационных ресурсов предприятия, например интеграция межсетевого экрана с VPN-шлюзом и транслятором IP-адресов.

По мере роста и развития КИС система информационной безопасности должна иметь возможность легко масштабироваться без потери целостности и управляемости. *Масштабируемость средств защиты* позволяет подбирать оптимальное по стоимости и надежности решение с возможностью постепенного наращивания системы защиты. Масштабирование обеспечивает эффективную работу предприятия при наличии у

него многочисленных филиалов, десятков предприятий-партнеров, сотен удаленных сотрудников и миллионов потенциальных клиентов.

Для того чтобы обеспечить надежную защиту ресурсов корпоративной информационной системы, в системе информационной безопасности должны быть реализованы самые прогрессивные и перспективные технологии информационной защиты. К ним относятся:

- *криптографическая защита данных* для обеспечения конфиденциальности, целостности и подлинности информации;
- *поддержка инфраструктуры управления открытыми ключами PKI*;
- *технологии аутентификации* для проверки подлинности пользователей и объектов сети путем применения одноразовых паролей, токенов (смарт-карт, USB-токенов) и других средств аутентификации;
- *управление доступом на уровне пользователей* и защита от несанкционированного доступа к информации;
- *защита электронного документооборота; баз данных и электронной почты*;
- *комплексный подход к обеспечению информационной безопасности*, обеспечивающий рациональное сочетание технологий и средств информационной защиты;
- *технологии межсетевых экранов* для защиты корпоративной сети от внешних угроз при подключении к общедоступным сетям связи;
- *технологии виртуальных защищенных каналов и сетей VPN* для защиты информации, передаваемой по открытым каналам связи;
- *технологии обнаружения и предотвращения вторжений в КИС*;
- *технологии защиты от вредоносных программ и спама* с использованием комплексов антивирусной защиты;
- *централизованное управление средствами информационной безопасности* на базе единой политики безопасности предприятия.

Учебное пособие «Комплексная защита информации в корпоративных системах» дает читателю достаточно полное представление о современных и перспективных методах, средствах и технологиях защиты информации в корпоративных системах и сетях.

Данная книга рекомендуется в качестве учебного пособия для студентов, обучающихся по направлению «Информатика и вычислительная техника». Книга представляет интерес для аспирантов и преподавателей соответствующих специальностей, а также пользователей и администраторов компьютерных сетей и систем, менеджеров, руководителей предприятий, заинтересованных в безопасности своих корпоративных информационных систем и сетей.

ЧАСТЬ I

ПРОБЛЕМЫ БЕЗОПАСНОСТИ КОРПОРАТИВНОЙ ИНФОРМАЦИИ

Корпоративные информационные системы (КИС) становятся сегодня одним из главных инструментов управления бизнесом и фактически важнейшим средством производства современной компании. Однако применение информационных технологий немыслимо без повышенного внимания к вопросам информационной безопасности. Разрушение информационного ресурса, его временная недоступность или несанкционированное использование могут нанести компании значительный материальный ущерб. Без должной степени защиты информации внедрение информационных технологий может оказаться экономически невыгодным в результате значительного ущерба из-за потерь конфиденциальных данных, хранящихся и обрабатываемых в компьютерных сетях.

Корпоративная информационная система представляет собой сложный комплекс разнородного аппаратного и программного обеспечения: компьютеров, операционных систем, сетевых средств, СУБД, разнообразных приложений. Все эти компоненты обычно обладают собственными средствами защиты, которые нужно согласовать между собой. Поэтому очень важна эффективная политика безопасности в качестве согласованной платформы по обеспечению безопасности корпоративной системы.

В последние годы в связи с развитием компьютерных сетей и ростом спроса на электронные услуги ситуация в сфере информационной безопасности серьезно обострилась, а вопрос стандартизации подходов к решению проблемы информационной безопасности стал особенно актуальным.

Реализация решений, обеспечивающих безопасность информационных ресурсов, существенно повышает эффективность всего процесса информатизации в организации, обеспечивая целостность, подлинность и конфиденциальность важной деловой информации, циркулирующей в локальных и глобальной информационных средах.

Глава 1
ОСНОВНЫЕ ПОНЯТИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Новые информационные технологии активно внедряются во все сферы человеческой деятельности. Появление локальных и глобальных сетей передачи данных предоставило пользователям компьютеров новые возможности для оперативного обмена информацией. Развитие Интернета привело к использованию глобальных сетей передачи данных в повседневной жизни практически каждого человека. По мере развития и усложнения средств, методов и форм автоматизации процессов обработки информации повышается зависимость общества от степени безопасности используемых им информационных технологий.

1.1. Основные понятия защиты информации и информационной безопасности

Современные методы обработки, передачи и накопления информации способствовали появлению угроз, связанных с возможностью потери, искажения и раскрытия данных, адресованных или принадлежащих конечным пользователям. Поэтому обеспечение информационной безопасности компьютерных систем и сетей является одним из ведущих направлений развития информационных технологий.

Рассмотрим основные понятия защиты информации и информационной безопасности компьютерных систем и сетей с учетом определений стандарта ГОСТ Р 50922—96 [13, 55].

Защита информации — это деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

Объект защиты — информация, или носитель информации, или информационный процесс, в отношении которого необходимо обеспечивать защиту в соответствии с поставленной целью защиты информации.

Цель защиты информации — это желаемый результат защиты информации. Целью защиты информации может быть предотвращение нанесения ущерба собственнику, владельцу, пользователю информации в результате возможной утечки информации и/или несанкционированного и непреднамеренного воздействия на информацию.

Эффективность защиты информации — степень соответствия результатов защиты информации поставленной цели.

Защита информации от утечки — деятельность по предотвращению неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа к ней и от получения защищаемой информации злоумышленниками.

Защита информации от несанкционированного воздействия — деятельность по предотвращению воздействия на защищаемую информацию с нарушением установленных прав и/или правил на изменение информации, приводящего к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

Защита информации от непреднамеренного воздействия — деятельность по предотвращению воздействия на защищаемую информацию ошибок пользователя информацией, сбоя технических и программных средств информационных систем, а также природных явлений или иных не направленных на изменение информации воздействий, связанных с функционированием технических средств, систем или с деятельностью людей, приводящей к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

Защита информации от разглашения — деятельность по предотвращению несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации.

Защита информации от несанкционированного доступа (НСД) — деятельность по предотвращению получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации. Заинтересованным субъектом, осуществляющим несанкционированный доступ к защищаемой информации, может выступать государство, юридическое лицо, группа физических лиц, в том числе общественная организация, отдельное физическое лицо.

Система защиты информации — совокупность органов и/или исполнителей, используемая ими техника защиты информации, а также объекты защиты, организованные и функционирующие по правилам, установленным соответствующими правовыми, организационно-распорядительными и нормативными документами по защите информации.

Под *информационной безопасностью* понимают защищенность информации от незаконного ознакомления, преобразования и уничтожения, а также защищенность информационных ресурсов от воздействий, направленных на нарушение их работоспособности. Природа этих воздействий может быть самой разнообразной. Это и попытки проникновения злоумышленников, и ошибки персонала, и выход из строя аппаратных и программных средств, стихийные бедствия (землетрясение, ураган, пожар и т. п.).

Современная *автоматизированная система обработки информации (АС)* представляет собой сложную систему, состоящую из большого числа компонентов различной степени автономности, которые связаны

между собой и обмениваются данными. Практически каждый компонент может подвергнуться внешнему воздействию или выйти из строя. *Компоненты ИС* можно разбить на следующие группы:

- *аппаратные средства* — компьютеры и их составные части (процессоры, мониторы, терминалы, периферийные устройства — дисководы, принтеры, контроллеры, кабели, линии связи) и т. д.;
- *программное обеспечение* — приобретенные программы, исходные, объектные, загрузочные модули; операционные системы и системные программы (компиляторы, компоновщики и др.), утилиты, диагностические программы и т. д.;
- *данные* — информация, хранимая временно и постоянно, на магнитных носителях, печатная, архивы, системные журналы и т. д.;
- *персонал* — обслуживающий персонал и пользователи.

Одной из особенностей обеспечения информационной безопасности в ИС является то, что таким абстрактным понятиям, как информация, объекты и субъекты системы, ставятся в соответствие физические представления в компьютерной среде:

- *для представления информации — машинные носители информации* в виде внешних устройств компьютерных систем (терминалов, печатающих устройств, различных накопителей, линий и каналов связи), оперативной памяти, файлов, записей и т. д.;
- под *объектами системы* понимают пассивные компоненты системы, хранящие, принимающие или передающие информацию. Доступ к объекту означает доступ к содержащейся в нем информации;
- под *субъектами системы* понимают активные компоненты системы, которые могут стать причиной потока информации от объекта к субъекту или изменения состояния системы. В качестве субъектов могут выступать пользователи, активные программы и процессы.

Информационная безопасность компьютерных систем достигается обеспечением конфиденциальности, целостности и достоверности обрабатываемых данных, а также доступности и целостности информационных компонентов и ресурсов системы.

Перечисленные выше *базовые свойства информации* нуждаются в более полном толковании.

Конфиденциальность данных — это статус, предоставленный данным и определяющий требуемую степень их защиты. К конфиденциальным данным можно отнести, например, следующие: личную информацию пользователей; учетные записи (имена и пароли); данные о кредитных картах; данные о разработках и различные внутренние документы; бухгалтерские сведения. Конфиденциальная информация должна быть известна только допущенным и прошедшим проверку (авторизованным) субъектам системы (пользователям, процессам, программам). Для остальных субъектов системы эта информация должна быть неизвестной.

Установление градаций важности защиты защищаемой информации (объекта защиты) называют *категорированием защищаемой информации.*

Под *целостностью информации* понимается свойство информации сохранять свою структуру и/или содержание в процессе передачи и хра-

нения. Целостность информации обеспечивается в том случае, если данные в системе не отличаются в семантическом отношении от данных в исходных документах, т. е. если не произошло их случайного или преднамеренного искажения или разрушения. Обеспечение целостности данных является одной из сложных задач защиты информации.

Достоверность информации — свойство информации, выражающееся в строгой принадлежности субъекту, который является ее источником, либо тому субъекту, от которого эта информация принята.

Юридическая значимость информации означает, что документ, являющийся носителем информации, обладает юридической силой.

Доступность данных — работа пользователя с данными возможна только в том случае, если он имеет к ним доступ.

Доступ к информации — получение субъектом возможности ознакомления с информацией, в том числе при помощи технических средств.

Субъект доступа к информации — участник правоотношений в информационных процессах.

Оперативность доступа к информации — это способность информации или некоторого информационного ресурса быть доступными для конечного пользователя в соответствии с его оперативными потребностями.

Собственник информации — субъект, в полном объеме реализующий полномочия владения, пользования, распоряжения информацией в соответствии с законодательными актами.

Владелец информации — субъект, осуществляющий владение и пользование информацией и реализующий полномочия распоряжения в пределах прав, установленных законом и/или собственником информации.

Пользователь (потребитель) информации — субъект, пользующийся информацией, полученной от ее собственника, владельца или посредника в соответствии с установленными правами и правилами доступа к информации либо с их нарушением.

Право доступа к информации — совокупность правил доступа к информации, установленных правовыми документами или собственником, владельцем информации.

Правила доступа к информации — совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям.

Различают санкционированный и несанкционированный доступ к информации.

Санкционированный доступ к информации — это доступ к информации, не нарушающий установленные правила разграничения доступа. Правила разграничения доступа служат для регламентации права доступа к компонентам системы.

Несанкционированный доступ (НСД) к информации характеризуется нарушением установленных правил разграничения доступа. Лицо или процесс, осуществляющие несанкционированный доступ к информации, являются нарушителями правил разграничения доступа. Несанкционированный доступ является наиболее распространенным видом компьютерных нарушений.

Ответственным за защиту компьютерной системы от несанкционированного доступа к информации является *администратор защиты.*

Доступность информации подразумевает также *доступность компонента или ресурса* компьютерной системы, т. е. свойство компонента или ресурса быть доступным для законных субъектов системы. Вот примерный перечень ресурсов, которые должны быть доступны: принтеры; серверы; рабочие станции; данные пользователей; любые критические данные, необходимые для работы.

Целостность ресурса или компонента системы — это свойство ресурса или компонента быть неизменными в семантическом смысле при функционировании системы в условиях случайных или преднамеренных искажений либо разрушающих воздействий.

С допуском к информации и ресурсам системы связана группа таких важных понятий, как идентификация, аутентификация, авторизация.

С каждым субъектом системы (сети) связывают некоторую информацию (число, строка символов), идентифицирующую субъект. Эта информация является *идентификатором* субъекта системы (сети). Субъект, имеющий зарегистрированный идентификатор, является *законным (легальным) субъектом. Идентификация субъекта* — это процедура распознавания субъекта по его идентификатору. Идентификация выполняется при попытке субъекта войти в систему (сеть).

Следующим шагом взаимодействия системы с субъектом является аутентификация субъекта. *Аутентификация субъекта* — это проверка подлинности субъекта с данным идентификатором. Процедура аутентификации устанавливает, является ли субъект именно тем, кем он себя объявил.

После идентификации и аутентификации субъекта выполняют процедуру авторизации.

Авторизация субъекта — это процедура предоставления законному субъекту, успешно прошедшему идентификацию и аутентификацию, соответствующих полномочий и доступных ресурсов системы (сети).

Под *угрозой безопасности* ИС понимаются возможные действия, способные прямо или косвенно нанести ущерб ее безопасности. *Ущерб безопасности* подразумевает нарушение состояния защищенности информации, содержащейся и обрабатываемой в системе (сети).

С понятием угрозы безопасности тесно связано понятие уязвимости компьютерной системы (сети). *Уязвимость компьютерной системы* — это присущее системе неудачное свойство, которое может привести к реализации угрозы.

Атака на компьютерную систему — это поиск и/или использование злоумышленником той или иной уязвимости системы. Иными словами, атака — это реализация угрозы безопасности.

Противодействие угрозам безопасности является целью средств защиты компьютерных систем и сетей.

Защищенная система — это система со средствами защиты, которые успешно и эффективно противостоят угрозам безопасности.

Способ защиты информации — порядок и правила применения определенных принципов и средств защиты информации.

Средство защиты информации — техническое, программное средство, вещество и/или материал, предназначенные или используемые для защиты информации.

Комплекс средств защиты (КСЗ) представляет собой совокупность программных и технических средств, создаваемых и поддерживаемых для обеспечения информационной безопасности системы (сети). КСЗ создается и поддерживается в соответствии с принятой в данной организации политикой безопасности.

Техника защиты информации — средства защиты информации, средства контроля эффективности защиты информации, средства и системы управления, предназначенные для обеспечения защиты информации.

Корпоративные сети относятся к распределенным информационным системам (ИС), осуществляющим обработку информации. Обеспечение безопасности ИС предполагает организацию противодействия любому несанкционированному вторжению в процесс функционирования ИС, а также попыткам модификации, хищения, выведения из строя или разрушения ее компонентов, т. е. защиту всех компонентов ИС — аппаратных средств, программного обеспечения, данных и персонала. Конкретный подход к проблеме обеспечения безопасности основан на политике безопасности, разработанной для ИС.

Политика безопасности — это совокупность норм, правил и практических рекомендаций, регламентирующих работу средств защиты компьютерной системы от заданного множества угроз. Более подробные сведения о видах политики безопасности и процессе ее разработки приводятся в главах 2 и 3.

1.2. Анализ угроз информационной безопасности

Рассмотрение возможных угроз информационной безопасности проводится с целью определения полного набора требований к разрабатываемой системе защиты. Обычно под *угрозой* (в общем смысле) понимают потенциально возможное событие (воздействие, процесс или явление), которое может привести к нанесению ущерба чьим-либо интересам. Далее под *угрозой безопасности* информационной системы будем понимать возможность воздействия на ИС, которое прямо или косвенно может нанести ущерб ее безопасности.

В настоящее время известен достаточно обширный перечень угроз безопасности ИС, содержащий сотни позиций. Перечень угроз, оценки вероятностей их реализации, а также модель нарушителя служат основой для анализа риска реализации угроз и формулирования требований к системе защиты ИС. Кроме выявления возможных угроз, целесообразно проведение анализа этих угроз на основе их классификации по ряду признаков. Каждый из признаков классификации отражает одно из обобщенных требований к системе защиты. Угрозы, соответствую-

щие каждому признаку классификации, позволяют детализировать отражаемое этим признаком требование.

Необходимость классификации угроз безопасности ИС обусловлена тем, что хранимая и обрабатываемая информация в современных ИС подвержена воздействию чрезвычайно большого числа факторов, в силу чего становится невозможным формализовать задачу описания полного множества угроз. Поэтому для защищаемой системы обычно определяют не полный перечень угроз, а перечень классов угроз.

Классификация возможных угроз безопасности ИС может быть проведена по ряду базовых признаков [67, 73].

1. *По природе возникновения* различают:
   - *естественные угрозы*, вызванные воздействиями на ИС объективных физических процессов или стихийных природных явлений;
   - *искусственные угрозы* безопасности ИС, вызванные деятельностью человека.
2. *По степени преднамеренности* проявления различают:
   - *угрозы, вызванные ошибками или халатностью* персонала, например некомпетентное использование средств защиты; ввод ошибочных данных и т. п.;
   - *угрозы преднамеренного действия*, например действия злоумышленников.
3. *По непосредственному источнику угроз.* Источниками угроз могут быть:
   - *природная среда*, например стихийные бедствия, магнитные бури и пр.;
   - *человек*, например вербовка путем подкупа персонала, разглашение конфиденциальных данных и т. п.;
   - *санкционированные программно-аппаратные средства*, например удаление данных, отказ в работе операционной системы;
   - *несанкционированные программно-аппаратные средства*, например заражение компьютера вирусами с деструктивными функциями.
4. *По положению источника угроз.* Источник угроз может быть расположен:
   - *вне контролируемой зоны ИС*, например перехват данных, передаваемых по каналам связи, перехват электромагнитных, акустических и других излучений устройств;
   - *в пределах контролируемой зоны ИС*, например применение подслушивающих устройств, хищение распечаток, записей, носителей информации и т. п.;
   - *непосредственно в ИС*, например некорректное использование ресурсов ИС.
5. *По степени зависимости от активности ИС.* Угрозы проявляются:
   - *независимо от активности ИС*, например вскрытие шифров криптозащиты информации;
   - *только в процессе обработки данных*, например угрозы выполнения и распространения программных вирусов.

6. *По степени воздействия на ИС* различают:
   - *пассивные угрозы*, которые при реализации ничего не меняют в структуре и содержании ИС, например угроза копирования секретных данных;
   - *активные угрозы*, которые при воздействии вносят изменения в структуру и содержание ИС, например внедрение троянских коней и вирусов.
7. *По этапам доступа пользователей или программ к ресурсам ИС* различают:
   - угрозы, проявляющиеся *на этапе доступа к ресурсам ИС*, например угрозы несанкционированного доступа в ИС;
   - угрозы, проявляющиеся *после разрешения доступа к ресурсам ИС*, например угрозы несанкционированного или некорректного использования ресурсов ИС.
8. *По способу доступа к ресурсам ИС* различают:
   - угрозы *с использованием стандартного пути доступа* к ресурсам ИС, например незаконное получение паролей и других реквизитов разграничения доступа с последующей маскировкой под зарегистрированного пользователя;
   - угрозы *с использованием скрытого нестандартного пути доступа* к ресурсам ИС, например несанкционированный доступ к ресурсам ИС путем использования недокументированных возможностей ОС.
9. *По текущему месту расположения информации, хранимой и обрабатываемой в ИС*, различают:
   - угрозы доступа к информации *на внешних запоминающих устройствах*, например несанкционированное копирование секретной информации с жесткого диска;
   - угрозы доступа к информации *в оперативной памяти*, например чтение остаточной информации из оперативной памяти; доступ к системной области оперативной памяти со стороны прикладных программ;
   - угрозы доступа к информации, циркулирующей *в линиях связи*, например незаконное подключение к линиям связи с последующим вводом ложных сообщений или модификацией передаваемых сообщений; незаконное подключение к линиям связи с целью прямой подмены законного пользователя с последующим вводом дезинформации и навязыванием ложных сообщений;
   - угрозы доступа к информации, отображаемой *на терминале или печатаемой на принтере*; например запись отображаемой информации на скрытую видеокамеру.

Как уже отмечалось, опасные воздействия на ИС подразделяют на случайные и преднамеренные. Анализ опыта проектирования, изготовления и эксплуатации ИС показывает, что информация подвергается различным случайным воздействиям на всех этапах цикла жизни и функционирования ИС.

Причинами *случайных воздействий* при эксплуатации ИС могут быть:

- аварийные ситуации из-за стихийных бедствий и отключений электропитания;
- отказы и сбои аппаратуры;
- ошибки в программном обеспечении;
- ошибки в работе обслуживающего персонала и пользователей;
- помехи в линиях связи из-за воздействий внешней среды.

Ошибки в программном обеспечении (ПО) являются распространенным видом компьютерных нарушений. Программное обеспечение серверов, рабочих станций, маршрутизаторов и т. д. написано людьми, поэтому оно практически всегда содержит ошибки. Чем выше сложность подобного программного обеспечения, тем больше вероятность обнаружения в нем ошибок и уязвимостей. Большинство из них не представляют никакой опасности, некоторые же могут привести к серьезным последствиям, таким как получение злоумышленником контроля над сервером, неработоспособность сервера, несанкционированное использование ресурсов (использование компьютера в качестве плацдарма для атаки и т. п.). Обычно подобные ошибки устраняются с помощью пакетов обновлений, регулярно выпускаемых производителем ПО. Своевременная установка таких пакетов является необходимым условием безопасности информации.

Преднамеренные угрозы связаны с целенаправленными действиями нарушителя. В качестве нарушителя могут выступать служащий, посетитель, конкурент, наемник и т. д. Действия нарушителя могут быть обусловлены разными мотивами: недовольством служащего своей карьерой, сугубо материальным интересом (взятка), любопытством, конкурентной борьбой, стремлением самоутвердиться любой ценой и т. п.

Исходя из возможности возникновения наиболее опасной ситуации, обусловленной действиями нарушителя, можно составить *гипотетическую модель потенциального нарушителя*:

- квалификация нарушителя может быть на уровне разработчика данной системы;
- нарушителем может быть как постороннее лицо, так и законный пользователь системы;
- нарушителю известна информация о принципах работы системы;
- нарушитель выберет наиболее слабое звено в защите.

В частности, для банковских ИС можно выделить следующие преднамеренные угрозы:

- несанкционированный доступ посторонних лиц, не принадлежащих к числу банковских служащих, и ознакомление с хранимой конфиденциальной информацией;
- ознакомление банковских служащих с информацией, к которой они не должны иметь доступ;
- несанкционированное копирование программ и данных;
- кража магнитных носителей, содержащих конфиденциальную информацию;
- кража распечатанных банковских документов;

- умышленное уничтожение информации;
- несанкционированная модификация банковскими служащими финансовых документов, отчетности и баз данных;
- фальсификация сообщений, передаваемых по каналам связи;
- отказ от авторства сообщения, переданного по каналам связи;
- отказ от факта получения информации;
- навязывание ранее переданного сообщения;
- разрушение информации, вызванное вирусными воздействиями;
- разрушение архивной банковской информации, хранящейся на магнитных носителях;
- кража оборудования.

Наиболее распространенным и многообразным видом компьютерных нарушений является *несанкционированный доступ (НСД)*. Суть НСД состоит в получении пользователем (нарушителем) доступа к объекту в нарушение правил разграничения доступа, установленных в соответствии с принятой в организации политикой безопасности. НСД использует любую ошибку в системе защиты и возможен при нерациональном выборе средств защиты, их некорректной установке и настройке. НСД может быть осуществлен как штатными средствами ИС, так и специально созданными аппаратными и программными средствами.

Перечислим основные каналы несанкционированного доступа, через которые нарушитель может получить доступ к компонентам ИС и осуществить хищение, модификацию и/или разрушение информации:

- штатные каналы доступа к информации (терминалы пользователей; оператора, администратора системы; средства отображения и документирования информации; каналы связи) при их использовании нарушителями, а также законными пользователями вне пределов их полномочий;
- технологические пульты управления;
- линии связи между аппаратными средствами ИС;
- побочные электромагнитные излучения от аппаратуры, линий связи, сетей электропитания и заземления и др.

Из всего разнообразия способов и приемов несанкционированного доступа остановимся на следующих распространенных и связанных между собой нарушениях:

- перехват паролей;
- маскарад;
- незаконное использование привилегий.

Перехват паролей осуществляется специально разработанными программами. При попытке законного пользователя войти в систему программа-перехватчик имитирует на экране дисплея ввод имени и пароля пользователя, которые сразу пересылаются владельцу программы-перехватчика, после чего на экран выводится сообщение об ошибке и управление возвращается операционной системе. Пользователь предполагает, что допустил ошибку при вводе пароля. Он повторяет ввод и получает доступ в систему. Владелец программы-перехватчика, получивший имя

и пароль законного пользователя, может теперь использовать их в своих целях. Существуют и другие способы перехвата паролей.

Маскарад — это выполнение каких-либо действий одним пользователем от имени другого пользователя, обладающего соответствующими полномочиями. Целью маскарада является приписывание каких-либо действий другому пользователю либо присвоение полномочий и привилегий другого пользователя. Примерами реализации маскарада являются:

- вход в систему под именем и паролем другого пользователя (этому маскараду предшествует перехват пароля);
- передача сообщений в сети от имени другого пользователя.

Маскарад особенно опасен в банковских системах электронных платежей, где неправильная идентификация клиента из-за маскарада злоумышленника может привести к большим убыткам законного клиента банка.

Незаконное использование привилегий. Большинство систем защиты устанавливают определенные наборы привилегий для выполнения заданных функций. Каждый пользователь получает свой набор привилегий: обычные пользователи — минимальный, администраторы — максимальный. Несанкционированный захват привилегий, например посредством маскарада, приводит к возможности выполнения нарушителем определенных действий в обход системы защиты. Следует отметить, что незаконный захват привилегий возможен либо при наличии ошибок в системе защиты, либо из-за халатности администратора при управлении системой и назначении привилегий.

Вредоносные программы. К таким программам относятся компьютерные вирусы, сетевые черви, программа «троянский конь». Особенно уязвимы к этим программам рабочие станции конечных пользователей. Дадим краткую характеристику этих распространенных угроз безопасности ИС.

Троянский конь представляет собой программу, которая наряду с действиями, описанными в ее документации, выполняет некоторые другие действия, ведущие к нарушению безопасности системы и деструктивным результатам. Аналогия такой программы с древнегреческим троянским конем вполне оправданна, так как в обоих случаях не вызывающая подозрений оболочка таит серьезную угрозу. Радикальный способ защиты от этой угрозы заключается в создании замкнутой среды исполнения программ, которые должны храниться и защищаться от несанкционированного доступа.

Компьютерный вирус представляет собой своеобразное явление, возникшее в процессе развития компьютерной и информационной техники. Суть этого явления состоит в том, что программы-вирусы обладают рядом свойств, присущих живым организмам, — они рождаются, размножаются и умирают. Термин «вирус» в применении к компьютерам предложил Фред Коэн из Университета Южной Калифорнии. Исторически первое определение вируса было дано также Ф. Коэном: «Компьютерный вирус — это программа, которая может заражать другие программы, модифицируя их посредством включения в них своей, возможно,

измененной копии, причем последняя сохраняет способность к дальнейшему размножению». Компьютерные вирусы наносят ущерб системе за счет быстрого размножения и разрушения среды обитания.

Сетевой червь является разновидностью программы-вируса, которая распространяется по глобальной сети. Следует отметить, что троянские кони, компьютерные вирусы и сетевые черви относятся к весьма опасным угрозам ИС.

Особенностью современных вредоносных программ является их ориентация на конкретное прикладное ПО, ставшее стандартом де-факто для большинства пользователей, в первую очередь это Microsoft Internet Explorer и Microsoft Outlook. Массовое создание вирусов под продукты «Майкрософт» объясняется не только низким уровнем безопасности и надежности программ, важную роль играет глобальное распространение этих продуктов. Авторы вредоносного программного обеспечения все активнее начинают исследовать «дыры» в популярных СУБД, связующих ПО и корпоративные бизнес-приложения, построенные на базе этих систем.

Вредоносные программы постоянно эволюционируют, основной тенденцией их развития является полиморфизм. Сегодня уже довольно сложно провести границу между вирусом, червем и троянской программой — они используют практически одни и те же механизмы, небольшая разница заключается лишь в степени этого использования. Устройство вредоносного программного обеспечения стало сегодня настолько унифицированным, что, например, отличить почтовый вирус от червя с деструктивными функциями практически невозможно. Даже в троянских программах появилась функция репликации (как одно из средств противодействия антивирусным средствам), так что при желании их вполне можно назвать вирусами (с механизмом распространения в виде маскировки под прикладные программы).

Для защиты от вредоносных программ необходимо применение ряда мер:

- исключение несанкционированного доступа к исполняемым файлам;
- тестирование приобретаемых программных средств;
- контроль целостности исполняемых файлов и системных областей;
- создание замкнутой среды исполнения программ.

Борьба с вирусами, червями и троянскими конями ведется с помощью эффективного антивирусного программного обеспечения, работающего на пользовательском уровне и на уровне сети. По мере появления новых вирусов, червей и троянских коней нужно устанавливать новые базы данных антивирусных средств и приложений. Подробная классификация и характеристика вредоносных программ приводится в главе 14, посвященной защите от них.

К непрограммным угрозам относятся спам, фишинг и фарминг. Распространенность этих угроз в последнее время значительно выросла.

Спам, объем которого сейчас превышает 80 % от общего объема почтового трафика, может создавать угрозу доступности информации,

блокируя почтовые серверы, либо использоваться для распространения вредоносного программного обеспечения.

Фишинг (Phishing) является относительно новым видом интернет-мошенничества, цель которого — получить идентификационные данные пользователей. Сюда относятся кражи паролей, номеров кредитных карт, банковских счетов, PIN-кодов и другой конфиденциальной информации, дающей доступ к деньгам пользователя. Фишинг использует не технические недостатки программного обеспечения, а легковерность пользователей Интернета. Сам термин phishing, созвучный с fishing (рыбная ловля), расшифровывается как password harvesting fishing — выуживание пароля. Действительно, фишинг очень похож на рыбную ловлю. Злоумышленник закидывает в Интернет приманку и «вылавливает» всех «рыбок» — пользователей Интернета, которые клюнут на эту приманку.

Злоумышленником создается практически точная копия сайта выбранного банка (электронной платежной системы, аукциона и т. п.). Затем при помощи спам-технологии по электронной почте рассылается письмо, составленное таким образом, чтобы быть максимально похожим на настоящее письмо от выбранного банка. При составлении письма используются логотипы банка, имена и фамилии реальных руководителей банка. В таком письме, как правило, сообщается о том, что из-за смены программного обеспечения в системе интернет-банкинга пользователю необходимо подтвердить или изменить свои учетные данные. В качестве причины для изменения данных могут быть названы выход из строя ПО банка или же нападение хакеров. Наличие правдоподобной легенды, побуждающей пользователя к необходимым действиям, — непременная составляющая успеха мошенников-фишеров. Во всех случаях цель таких писем одна — заставить пользователя щелкнуть по приведенной ссылке, а затем ввести свои конфиденциальные данные (пароль, номер счета, PIN-код) на ложном сайте банка (электронной платежной системы, аукциона). Зайдя на ложный сайт, пользователь вводит в соответствующие строки свои конфиденциальные данные, а далее аферисты получают доступ в лучшем случае к его почтовому ящику, а в худшем — к электронному счету.

Технологии фишеров совершенствуются, применяются методы социальной инженерии. Клиента пытаются напугать, придумать критичную причину для того, чтобы он выдал свои конфиденциальные данные. Как правило, сообщения содержат угрозы, например, заблокировать счет в случае невыполнения получателем требований, изложенных в сообщении.

В настоящее время мошенники часто используют троянские программы. Задача фишера в этом случае сильно упрощается — достаточно заставить пользователя перебраться на фишерский сайт и «подцепить» программу, которая самостоятельно разыщет на винчестере жертвы все, что нужно. Наравне с троянскими программами стали использоваться и кейлоггеры. На подставных сайтах на компьютеры жертв загружают шпионские утилиты, отслеживающие нажатия клавиш. При использовании такого подхода необязательно находить выходы на клиентов кон-

кретного банка или компании, а потому фишеры стали подделывать и сайты общего назначения, такие как новостные ленты и поисковые системы.

Успеху фишинг-афер способствует низкий уровень осведомленности пользователей о правилах работы компаний, от имени которых действуют преступники. В частности, около 5 % пользователей не знают простого факта: банки не рассылают писем с просьбой подтвердить в онлайне номер своей кредитной карты и ее PIN-код.

Появилось сопряженное с фишингом понятие — фарминг.

Фарминг (Pharming) — это еще один вид мошенничества, ставящий целью получить персональные данные пользователей, но не через почту, а прямо через официальные веб-сайты. Фармеры заменяют на серверах DNS цифровые адреса легитимных веб-сайтов на поддельные, в результате чего пользователи перенаправляются на сайты мошенников. Этот вид мошенничества еще опаснее, так как заметить подделку практически невозможно.

Основной защитой от фишинга пока остаются спам-фильтры. К сожалению, программный инструментарий для защиты от фишинга обладает ограниченной эффективностью, поскольку злоумышленники эксплуатируют в первую очередь не бреши в ПО, а человеческую психологию. Активно разрабатываются технические средства безопасности, прежде всего плагины для популярных браузеров. Суть защиты заключается в блокировании сайтов, попавших в черные списки мошеннических ресурсов. Следующим шагом могут стать системы генерации одноразовых паролей для интернет-доступа к банковским счетам и аккаунтам в платежных системах, повсеместное распространение дополнительных уровней защиты за счет комбинации ввода пароля с использованием аппаратного USB-ключа.

Принято считать, что, вне зависимости от конкретных видов угроз или их проблемно-ориентированной классификации, ИС удовлетворяет потребности эксплуатирующих ее лиц, если обеспечиваются следующие важные свойства информации и систем ее обработки: *конфиденциальность, целостность и доступность информации.*

Иными словами, в соответствии с существующими подходами считают, что информационная безопасность ИС обеспечена в случае, если для информационных ресурсов в системе поддерживаются определенные уровни:

- конфиденциальности (невозможности несанкционированного получения какой-либо информации);
- целостности (невозможности несанкционированной или случайной ее модификации);
- доступности (возможности за разумное время получить требуемую информацию).

Соответственно, для автоматизированных информационных систем рассматривают три основных вида угроз:

- *угрозы нарушения конфиденциальности*, направленные на разглашение конфиденциальной или секретной информации. При реа-

лизации этих угроз информация становится известной лицам, которые не должны иметь к ней доступ. В терминах компьютерной безопасности угроза нарушения конфиденциальности имеет место всякий раз, когда получен несанкционированный доступ к некоторой закрытой информации, хранящейся в компьютерной системе или передаваемой от одной системы к другой;

- *угрозы нарушения целостности информации*, хранящейся в компьютерной системе или передаваемой по каналу связи, которые направлены на ее изменение или искажение, приводящее к нарушению ее качества или полному уничтожению. Целостность информации может быть нарушена умышленно злоумышленником, а также в результате объективных воздействий со стороны среды, окружающей систему. Эта угроза особенно актуальна для систем передачи информации — компьютерных сетей и систем телекоммуникаций. Умышленные нарушения целостности информации не следует путать с ее санкционированным изменением, которое выполняется полномочными лицами с обоснованной целью (например, таким изменением является периодическая коррекция какой-либо базы данных);
- *угрозы нарушения работоспособности (отказ в обслуживании)*, направленные на создание таких ситуаций, когда определенные преднамеренные действия либо снижают работоспособность ИС, либо блокируют доступ к некоторым ее ресурсам. Например, если один пользователь системы запрашивает доступ к некоторой службе, а другой предпринимает действия по блокированию этого доступа, то первый пользователь получает отказ в обслуживании. Блокирование доступа к ресурсу может быть постоянным или временным.

Данные виды угроз можно считать первичными, или непосредственными, поскольку реализация этих угроз ведет к непосредственному воздействию на защищаемую информацию.

Для современных информационных технологий подсистемы защиты являются неотъемлемой частью ИС обработки информации. Атакующая сторона должна преодолеть эту подсистему защиты, чтобы нарушить, например, конфиденциальность ИС. Однако нужно сознавать, что не существует абсолютно стойкой системы защиты, — вопрос лишь во времени и средствах, требующихся на ее преодоление. Исходя из данных условий, рассмотрим следующую модель: защита информационной системы считается преодоленной, если в ходе исследования этой системы определены все ее уязвимости.

Преодоление защиты также представляет собой угрозу, поэтому для защищенных систем можно рассматривать четвертый вид угрозы — *угрозу раскрытия параметров ИС*, включающей в себя подсистему защиты. На практике любое проводимое мероприятие предваряется этапом разведки, в ходе которого определяются основные параметры системы, ее характеристики и т. п. Результатом этого этапа является уточнение поставленной задачи, а также выбор наиболее оптимального технического средства.

Угрозу раскрытия параметров ИС можно считать опосредованной. Последствия ее реализации не причиняют какого-либо ущерба обрабатываемой информации, но дают возможность реализовать первичные, или непосредственные, угрозы, перечисленные выше.

При рассмотрении вопросов защиты ИС целесообразно использовать четырехуровневую градацию доступа к хранимой, обрабатываемой и защищаемой ИС информации. Такая градация доступа поможет систематизировать как возможные угрозы, так и меры по их нейтрализации и парированию, т. е. поможет систематизировать весь спектр методов обеспечения защиты, относящихся к информационной безопасности.

Эти уровни доступа следующие:

- уровень носителей информации;
- уровень средств взаимодействия с носителем;
- уровень представления информации;
- уровень содержания информации.

Введение данных уровней обусловлено следующими соображениями.

Во-первых, информация для удобства манипулирования чаще всего фиксируется на некотором материальном носителе, которым может быть дискета или что-нибудь подобное.

Во-вторых, если способ представления информации таков, что она не может быть непосредственно воспринята человеком, возникает необходимость в преобразователях информации в доступный для человека способ представления. Например, для чтения информации с дискеты необходим компьютер, оборудованный дисководом соответствующего типа.

В-третьих, как уже было отмечено, информация может быть охарактеризована способом своего представления, или тем, что еще называется языком в обиходном смысле. Язык символов, язык жестов и т. п. — все это способы представления информации.

В-четвертых, человеку должен быть доступен смысл представленной информации, ее семантика.

К основным направлениям реализации злоумышленником информационных *угроз* относятся:

- непосредственное обращение к объектам доступа;
- создание программных и технических средств, выполняющих обращение к объектам доступа в обход средств защиты;
- модификация средств защиты, позволяющая реализовать угрозы информационной безопасности;
- внедрение в технические средства ИС программных или технических механизмов, нарушающих предполагаемую структуру и функции ИС.

В табл. 1.1 перечислены основные методы реализации угроз информационной безопасности.

Для достижения требуемого уровня информационной безопасности ИС необходимо обеспечить противодействие различным техническим угрозам и минимизировать возможное влияние человеческого фактора.

Таблица 1.1. **Основные методы реализации угроз информационной безопасности**

	Методы реализации угроз информационной безопасности			
Уровень доступа к информации в ИС	Угроза раскрытия параметров системы	Угроза нарушения конфиденциальности	Угроза нарушения целостности	Угроза отказа служб (отказа доступа к информации)
Уровень носителей информации	Определение типа и параметров носителей информации	Хищение (копирование) носителей информации	Уничтожение машинных носителей информации	Выведение из строя машинных носителей информации
Уровень средств взаимодействия с носителем	Получение информации о программно-аппаратной среде. Получение детальной информации о функциях, выполняемых ИС. Получение данных о применяемых системах защиты	Несанкционированный доступ к ресурсам ИС. Совершение пользователем несанкционированных действий. Несанкционированное копирование программного обеспечения. Перехват данных, передаваемых по каналам связи	Внесение пользователем несанкционированных изменений в программы и данные. Установка и использование нештатного программного обеспечения. Заражение программными вирусами	Проявление ошибок проектирования и разработки программно-аппаратных компонентов ИС. Обход механизмов защиты ИС
Уровень представления информации	Определение способа представления информации	Визуальное наблюдение. Раскрытие представления информации (дешифрование)	Внесение искажения в представление данных. Уничтожение данных	Искажение соответствия синтаксических и семантических конструкций языка
Уровень содержания информации	Определение содержания данных на качественном уровне	Раскрытие содержания информации	Внедрение дезинформации	Запрет на использование информации

Рассмотрим *тенденции развития ИТ-угроз.* По мере развития и усложнения ИТ-инфраструктуры автоматически растет количество потенциальных ИТ-угроз и рисков. Кроме того, угрозы становятся все более изощренными, поскольку хакеры, спамеры и иные злоумышленники активно берут на вооружение возможности, открывающиеся по мере развития информационных технологий.

Возрастание опасности внутренних ИТ-угроз. Традиционно наиболее опасными считались внешние угрозы (в первую очередь вирусы), защите от которых уделялось особое внимание. Однако постепенно все больше возрастает опасность внутренних ИТ-угроз. В 2007 г. инсайдерские угрозы впервые опередили вирусные, ранее неизменно находившиеся в первой строчке рейтинга как по числу инцидентов, так и по объему причиняемого ущерба.

В отчете «Trends in IT Security Threats», подготовленном Computer Economics, на первой позиции фигурируют угрозы со стороны инсайдеров (табл. 1.2), опережающие по наносимому совокупному ущербу

(финансовым убыткам и падению репутации компании) прочие виды угроз. Второе место досталось спаму — произошел заметный рост данного типа угроз.

Таблица 1.2. **Десятка наиболее опасных ИТ-угроз (источник: Computer Economics)**

Позиция в рейтинге	ИТ-угроза
1	Угроза инсайдеров
2	Спам
3	Угрозы от вредоносных программ (компьютерные вирусы, черви, троянцы, spyware- и adware-модули)
4	Неавторизованный доступ со стороны внешних нарушителей
5	Угроза физической потери носителя информации
6	Электронное мошенничество
7	Фарминг-атаки
8	Фишинг-атаки
9	Электронный вандализм и саботаж
10	Атаки типа «отказ в обслуживании»

Угрозы от вредоносных программ занимают третье место в рейтинге, поскольку по-прежнему имеется немало организаций, где защита от подобных угроз пока реализована на недостаточном уровне.

На четвертом месте находится неавторизованный доступ со стороны внешних нарушителей, а на пятом — угроза физической потери носителя информации.

Расширение спектра ИТ-угроз. Сегодня все более серьезную угрозу для безопасности компаний представляют возрастающая мобильность пользователей (применение ноутбуков за пределами корпоративной сети стало практически повсеместным) и современные пользовательские информационные технологии (бесплатная почта, ICQ, чаты, блоги, Wi-Fi и пр.), все активнее проникающие в корпоративную сферу.

Мобильные устройства сотрудников и пользовательские информационные технологии (при всей своей полезности) представляют для компаний огромную опасность. Мобильные устройства вместе с находящейся на них корпоративной информацией нередко оказываются украденными или потерянными, причем часто находящаяся на них конфиденциальная информация никак не защищена. Кроме того, мобильные устройства и пользовательские технологии предоставляют множество способов скопировать конфиденциальную информацию, чем и пользуются инсайдеры.

Аналитики компании Gartner назвали мобильные устройства и пользовательские информационные технологии одной из наиболее существенных угроз корпоративной безопасности — и те и другие позволяют сотрудникам совершенно бесконтрольно копировать и распространять конфиденциальную информацию и увеличивают вероятность получить вирус или троян. В связи с этим компаниям следует органи-

зовать просмотр всего http- и peer-to-peer-трафика, блокировать подозрительные пакеты, контролировать использование мобильных носителей, ограничивать и контролировать удаленный доступ (в том числе беспроводной) и т. д.

Угрозы и уязвимости компьютерных сетей подробно рассматриваются в главе 2.

Вопросы для самоконтроля

1. Сформулируйте понятие информационной безопасности ИС.
2. Объясните понятия целостности, конфиденциальности и доступности информации.
3. Объясните понятия идентификации, аутентификации и авторизации пользователя. Как они взаимосвязаны?
4. Укажите отличия санкционированного доступа от несанкционированного доступа к информации.
5. Сформулируйте определение политики безопасности.
6. Объясните понятие «угроза безопасности ИС».
7. Укажите основные признаки классификации возможных угроз безопасности ИС.
8. Каковы основные виды угроз безопасности ИС по цели и степени воздействия?
9. Дайте краткую характеристику угрозы безопасности, обозначаемой термином «троянский конь».
10. Дайте краткую характеристику угроз безопасности, обозначаемых терминами «вирус» и «червь».
11. Перечислите основные методы реализации угроз информационной безопасности и дайте их краткую характеристику.

Глава 2
ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СЕТЕЙ

Основным свойством, отличающим компьютерные сети от автономных компьютеров, является наличие обмена информацией между сетевыми узлами, связанными линиями передачи данных.

Объединение компьютеров в компьютерные сети позволяет значительно повысить эффективность использования компьютерной системы в целом. Повышение эффективности при этом достигается за счет возможности обмена информацией между компьютерами сети, а также за счет возможности использования на каждом компьютере общих сетевых ресурсов (информации, внешней памяти, программных приложений, внешних устройств).

Одним из основных признаков корпоративной сети является применение глобальных связей для объединения отдельных локальных сетей филиалов предприятия и компьютеров его удаленных сотрудников с центральной локальной сетью.

Следует отметить, что в последние годы интенсивно развиваются беспроводные компьютерные сети, и в частности беспроводные локальные сети WLAN (Wireless Local Area Network).

2.1. Введение в сетевой информационный обмен

Стремительное развитие информационных технологий привело к появлению и быстрому росту глобальной сети Интернет. Развитие компьютерных сетей немыслимо без строгого соблюдения принципов стандартизации аппаратного и программного обеспечения. Днем рождения Интернета в современном понимании этого слова стала дата стандартизации в 1983 г. стека коммуникационных протоколов TCP/IP, лежащего в основе всемирной сети Интернет по нынешний день. Интернет является совокупностью соединенных между собой компьютерных сетей, в которых используются единые согласованные правила обмена данными между компьютерами.

2.1.1. Использование сети Интернет

Развитие глобальной сети Интернет способствовало использованию для построения глобальных корпоративных связей более дешевого и

более доступного (по сравнению с выделенными каналами) транспорта Интернета. Сеть Интернет предлагает разнообразные методы коммуникации и способы доступа к информации, поэтому для многих компаний она быстро становится неотъемлемой частью их информационной системы.

Кроме транспортных услуг по транзитной передаче данных для абонентов любых типов, сеть Интернет обеспечивает также достаточно широкий набор высокоуровневых сетевых сервисов (услуг). Компьютеры, предоставляющие эти услуги, называются *серверами,* соответственно компьютеры, пользующиеся услугами, называются *клиентами.* Эти же термины относятся и к программному обеспечению, используемому на компьютерах-серверах и компьютерах-клиентах.

Влияние Интернета на корпоративные сети способствовало появлению нового понятия — интранет (интрасети), при котором способы доставки и обработки информации, присущие Интернету, переносятся в корпоративную сеть.

Отметим основные возможности, предоставляемые сетью Интернет для построения корпоративных сетей [7].

Дешевые и доступные коммуникационные каналы Интернета. В последнее десятилетие в связи с бурным развитием Интернета и сетей коллективного доступа в мире произошел качественный скачок в распространении и доступности информации. Пользователи получили дешевые и доступные коммуникационные каналы Интернета. Стремясь к экономии средств, предприятия начинают активно использовать эти каналы для передачи критичной коммерческой и управленческой информации.

Универсальность. Глобальная сеть Интернет была создана для обеспечения обмена информацией между удаленными пользователями. Развитие интернет-технологий привело к возникновению популярной глобальной службы World Wide Web (WWW), что позволило пользователям работать с информацией в режиме прямого подключения. Данная технология подразумевает подключение пользователя к Глобальной сети и использования WWW-браузеров для просмотра информации. Стандартизация интерфейсов обмена данными между утилитами просмотра информации и информационными серверами позволила организовать одинаковый интерфейс с пользователем для различных платформ.

Доступ к разнообразной информации и услугам в Интернете. Кроме транспортных услуг по транзитной передаче данных для абонентов любых типов, сеть Интернет обеспечивает также достаточно широкий набор высокоуровневых интернет-сервисов: Всемирная паутина (World Wide Web); сервис имен доменов DNS; доступ к файловым архивам FTP; электронная почта (e-mail); телеконференции (Usenet); сервисы общения ICQ, IRC; сервис Telnet; поиск информации в Интернете. Сеть Интернет обеспечивает доступ к обширной и разнообразной информации с помощью огромного числа подключенных к ней хост-узлов. *Хост* — это компьютер или группа компьютеров, имеющих прямое сетевое соединение с Интернетом и предоставляющих пользователям

доступ к своим средствам и службам. Многие из этих компьютеров выполняют роль серверов, предлагающих любому пользователю, имеющему выход в Интернет, доступ к электронным ресурсам — данным, приложениям и услугам. Связав свои сети с внешними ресурсами, компании могут реализовать постоянные коммуникации и организовать эффективный поток информации между людьми. Соединение внутренних сетей с внешними организациями и ресурсами позволяет компаниям воспользоваться преимуществами этих сетей — снижением затрат и повышением эффективности.

Простота использования. При использовании интернет-технологий не требуется специального обучения персонала.

Для объединения локальных сетей в глобальные используются специализированные компьютеры (маршрутизаторы и шлюзы), с помощью которых локальные сети подключаются к межсетевым каналам связи. Маршрутизаторы и шлюзы физически соединяют локальные сети друг с другом и, используя специальное программное обеспечение, передают данные из одной сети в другую. Глобальные сети имеют сложную разветвленную структуру и избыточные связи. Маршрутизаторы и шлюзы обеспечивают поиск оптимального маршрута при передаче данных в глобальных сетях, благодаря чему достигается максимальная скорость потока сообщений. Высокоскоростные каналы связи между локальными сетями могут быть реализованы на основе волоконно-оптических кабелей или с помощью спутниковой связи. В качестве медленных межсетевых каналов связи используются различные виды телефонных линий.

Построение корпоративных компьютерных сетей с применением технологии интрасетей означает, прежде всего, использование стека TCP/IP для транспортировки данных и технологии Web для их представления.

2.1.2. Модель ISO/OSI и стек протоколов TCP/IP

Основная задача, решаемая при создании компьютерных сетей, — обеспечение совместимости оборудования по электрическим и механическим характеристикам и совместимости информационного обеспечения (программ и данных) по системам кодирования и формату данных. Решение этой задачи относится к области стандартизации. Методологической основой стандартизации в компьютерных сетях является многоуровневый подход к разработке средств сетевого взаимодействия.

На основе этого подхода и технических предложений Международного института стандартов ISO (International Standards Organization) в начале 1980-х годов была разработана *стандартная модель взаимодействия открытых систем OSI (Open Systems Interconnection).* Модель ISO/OSI сыграла важную роль в развитии компьютерных сетей.

Модель OSI определяет различные уровни взаимодействия систем и указывает, какие функции должен выполнять каждый уровень. В моде-

ли OSI средства взаимодействия делятся на семь уровней: прикладной (Application), представительный (Presentation), сеансовый (Session), транспортный (Transport), сетевой (Network), канальный (Data Link) и физический (Physical). Самый верхний уровень — прикладной. На этом уровне пользователь взаимодействует с приложениями. Самый нижний уровень — физический. Этот уровень обеспечивает обмен сигналами между устройствами.

Обмен данными через каналы связи происходит путем перемещения данных с верхнего уровня на нижний, затем транспортировки по линиям связи и, наконец, обратным воспроизведением данных в компьютере клиента в результате их перемещения с нижнего уровня на верхний.

Для обеспечения необходимой совместимости на каждом из уровней архитектуры компьютерной сети действуют *специальные стандартные протоколы.* Они представляют собой формализованные правила, определяющие последовательность и формат сообщений, которыми обмениваются сетевые компоненты, лежащие на одном уровне, но в разных узлах сети.

Иерархически организованный набор протоколов, достаточный для организации взаимодействия узлов в сети, называется *стеком коммуникационных протоколов.* Следует четко различать модель ISO/OSI и стек протоколов ISO/OSI. *Модель ISO/OSI* является концептуальной схемой взаимодействия открытых систем, а *стек протоколов ISO/OSI* представляет собой набор вполне конкретных спецификаций протоколов для семи уровней взаимодействия, которые определены в модели ISO/OSI.

Коммуникационные протоколы могут быть реализованы как программно, так и аппаратно. Протоколы нижних уровней часто реализуются комбинацией программных и аппаратных средств, а протоколы верхних уровней — как правило, чисто программными средствами.

Модули, реализующие протоколы соседних уровней и находящиеся в одном узле сети, должны взаимодействовать друг с другом также в соответствии с четко определенными правилами и с помощью стандартизованных форматов сообщений. Эти правила принято называть *межуровневым интерфейсом.* Межуровневый интерфейс определяет набор сервисов, предоставляемых данным уровнем соседнему уровню. В сущности, протокол и интерфейс являются близкими понятиями, но традиционно в сетях за ними закреплены разные области действия: *протоколы* определяют правила взаимодействия модулей одного уровня в разных узлах сети, а *интерфейсы* определяют правила взаимодействия модулей соседних уровней в одном узле.

Стек протоколов TCP/IP (Transmission Control Protocol/Internet Protocol) является промышленным стандартом стека коммуникационных протоколов, разработанным для глобальных сетей. Стандарты TCP/IP опубликованы в серии документов, названных Request for Comment (RFC). Документы RFC описывают внутреннюю работу сети Интернет. Некоторые RFC описывают сетевые сервисы или протоколы и их реализацию, в то время как другие обобщают условия применения.

Стек TCP/IP объединяет в себе целый набор взаимодействующих между собой протоколов. Самыми важными из них являются протокол IP, отвечающий за поиск маршрута (или маршрутов) в Интернете от одного компьютера к другому через множество промежуточных сетей, шлюзов и маршрутизаторов и передачу блоков данных по этим маршрутам, и протокол TCP, обеспечивающий надежную доставку, безошибочность и правильный порядок приема передаваемых данных.

Большой вклад в развитие стека TCP/IP внес Калифорнийский университет в Беркли (США), который реализовал протоколы стека в своей версии ОС UNIX, сделав как сами программы, так и их исходные тексты бесплатными и общедоступными. Популярность этой операционной системы привела к широкому распространению IP, TCP и других протоколов стека.

Сегодня этот стек используется для связи компьютеров всемирной информационной сети Интернет, а также в огромном числе корпоративных сетей. Стек TCP/IP является самым распространенным средством организации составных компьютерных сетей.

Широкое распространение стека TCP/IP объясняется следующими его свойствами:

- наиболее завершенный стандартный и в то же время популярный стек сетевых протоколов, имеющий многолетнюю историю;
- почти все большие сети передают основную часть своего трафика с помощью протокола TCP/IP;
- все современные операционные системы поддерживают стек TCP/IP;
- метод получения доступа к сети Интернет;
- гибкая технология для соединения разнородных систем на уровне как транспортных подсистем, так и прикладных сервисов;
- основа для создания корпоративной интранет-сети, использующей транспортные услуги Интернета и гипертекстовую технологию WWW, разработанную в Интернете;
- устойчивая масштабируемая межплатформенная среда для приложений клиент/сервер [40].

Структура и функциональность стека протоколов TCP/IP

Стек TCP/IP был разработан до появления модели взаимодействия открытых систем OSI и также имеет многоуровневую структуру. Структура протоколов TCP/IP приведена на рис. 2.1. Стек протоколов TCP/IP имеет четыре уровня: прикладной (Application), транспортный (Transport), уровень межсетевого взаимодействия (Internet) и уровень сетевых интерфейсов (Network). Для сравнения на рис. 2.6 показаны также семь уровней модели OSI. Следует отметить, что соответствие уровней стека TCP/IP уровням модели OSI достаточно условно.

Прикладной уровень (Application) включает большое число прикладных протоколов и сервисов. К ним относятся такие популярные прото-

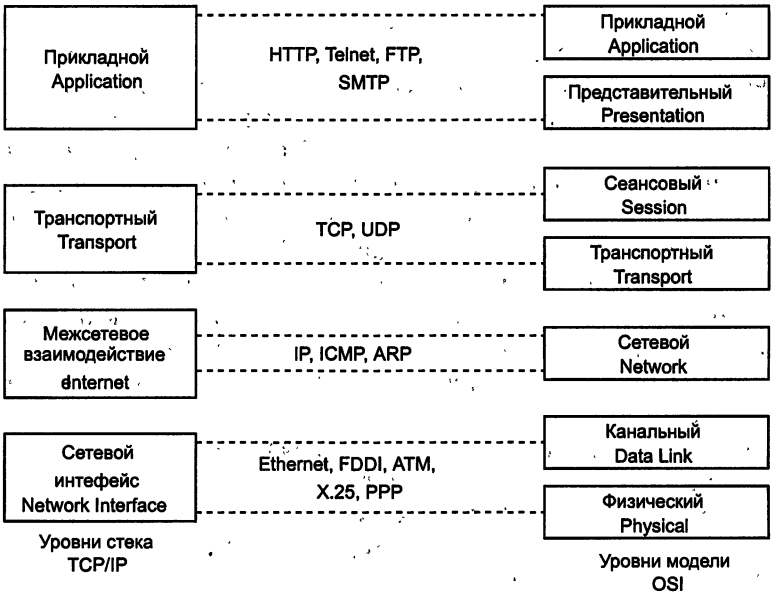


Рис. 2.1. Уровни стека протоколов TCP/IP

колы, как протокол копирования файлов FTP, протокол эмуляции терминала Telnet, почтовый протокол SMPT, используемый в электронной почте сети Интернет, гипертекстовые сервисы доступа к удаленной информации, например WWW, и многие другие. Рассмотрим несколько подробнее некоторые из этих протоколов [43].

Протокол пересылки файлов FTP (File Transfer Protocol) реализует удаленный доступ к файлу. Для того чтобы обеспечить надежную передачу, FTP использует в качестве транспорта протокол с установлением соединений — TCP. Кроме пересылки файлов протокол FTP предлагает и другие услуги. Например, пользователю предоставляется возможность интерактивной работы с удаленной машиной, в частности, он может распечатать содержимое ее каталогов. Наконец, FTP выполняет аутентификацию пользователей. Прежде чем получить доступ к файлу, в соответствии с протоколом пользователи должны сообщить свое имя и пароль. Для доступа к публичным каталогам FTP-архивов Интернета не требуется парольная аутентификация, и ее можно обойти путем использования для такого доступа предопределенного имени пользователя Anonymous.

В стеке TCP/IP протокол FTP предлагает наиболее широкий набор услуг для работы с файлами, однако он является и самым сложным для программирования. Если приложению не требуются все возможности протокола FTP, тогда можно использовать простой протокол пересылки файлов TFTP (Trivial File Transfer Protocol). Этот протокол реализует только передачу файлов, причем в качестве транспорта используется протокол без установления соединения — UDP.

Протокол Telnet обеспечивает передачу потока байтов между процессами, а также между процессом и терминалом. Наиболее часто этот

протокол используется для эмуляции терминала удаленного компьютера. При использовании сервиса Telnet пользователь фактически управляет удаленным компьютером так же, как и локальный пользователь, поэтому такой вид доступа требует хорошей защиты. Серверы Telnet всегда используют как минимум аутентификацию по паролю, а иногда и более мощные средства защиты, например систему Kerberos.

Протокол SNMP (Simple Network Management Protocol) используется для организации сетевого управления. Сначала протокол SNMP был разработан для удаленного контроля и управления маршрутизаторами Интернета. С ростом популярности протокол SNMP стали применять для управления разным коммуникационным оборудованием — концентраторами, мостами, сетевыми адаптерами и др. В стандарте SNMP определена спецификация информационной базы данных управления сетью. Эта спецификация, известная как база данных MIB (Management Information Base), определяет те элементы данных, которые управляемое устройство должно сохранять, и допустимые операции над ними.

На **транспортном уровне (Transport)** стека TCP/IP, называемом также основным уровнем, функционируют протоколы TCP и UDP.

Протокол управления передачей TCP (Transmission Control Protocol) решает задачу обеспечения надежной информационной связи между двумя конечными узлами. Этот протокол называют протоколом «с установлением соединения». Это означает, что два узла, связывающиеся при помощи этого протокола, «договариваются» о том, что они будут обмениваться потоком данных, и принимают некоторые соглашения об управлении этим потоком. Согласно протоколу TCP, отправляемые данные «нарезаются» на небольшие стандартные пакеты, после чего каждый пакет маркируется таким образом, чтобы в нем были данные для правильной сборки документа на компьютере получателя.

Протокол дейтаграмм пользователя UDP (User Datagram Protocol) обеспечивает передачу прикладных пакетов дейтаграммным способом, т. е. каждый блок передаваемой информации (пакет) обрабатывается и распространяется от узла к узлу как независимая единица информации — дейтаграмма. При этом протокол UDP выполняет только функции связующего звена между сетевым протоколом и многочисленными прикладными процессами. Необходимость в протоколе UDP обусловлена тем, что он «умеет» различать приложения и доставляет информацию от приложения к приложению.

Уровень межсетевого взаимодействия (Internet) реализует концепцию коммутации пакетов без установления соединений. Основным протоколом этого уровня является *адресный протокол IP*. Этот протокол изначально проектировался как протокол передачи пакетов в составных сетях, которые состоят из большого количества локальных сетей, объединенных как локальными, так и глобальными связями.

Суть протокола IP заключается в том, что у каждого пользователя всемирной сети Интернет должен быть свой уникальный адрес (IP-адрес). Без этого нельзя говорить о точной доставке TCP-пакетов в нуж-

ное место. Этот адрес выражается очень просто — четырьмя байтами, например 185.47.39.14. Структура IP-адреса организована таким образом, что каждый компьютер, через который проходит какой-либо TCP-пакет, может по этим четырем числам определить, кому из ближайших «соседей» надо переслать пакет, чтобы он оказался «ближе» к получателю. В результате конечного числа перебросок TCP-пакет достигает адресата. В данном случае оценивается не географическая близость. В расчет принимаются условия связи и пропускная способность линии. Два компьютера, находящиеся на разных континентах, но связанные высокопроизводительной линией космической связи, считаются более близкими друг другу, чем два компьютера из соседних городов, связанных обычной телефонной связью. Решением вопросов, что считать «ближе», а что «дальше», занимаются специальные средства — маршрутизаторы. Роль маршрутизатора в сети может выполнять как специализированный компьютер, так и специализированная программа, работающая на узловом сервере сети.

К уровню межсетевого взаимодействия относятся и протоколы, связанные с составлением и модификацией таблиц маршрутизации, такие как *протоколы сбора маршрутной информации RIP (Routing Internet Protocol)* и *OSPF (Open Shortest Path First)*, а также *протокол межсетевых управляющих сообщений ICMP (Internet Control Message Protocol)*. Последний протокол предназначен для обмена информацией об ошибках между маршрутизаторами сети и узлом — источником пакета.

Уровень сетевого интерфейса (Network) соответствует физическому и канальному уровням модели OSI. Этот уровень в протоколах TCP/IP не регламентируется, но поддерживает все популярные стандарты физического и канального уровня: для локальных сетей это Ethernet, Token Ring, FDDI, Fast Ethernet, для глобальных сетей — протоколы соединений точка—точка SLIP и PPP, протоколы территориальных сетей с коммутацией пакетов X.25, Frame Relay. Разработана спецификация, определяющая использование технологии ATM в качестве транспорта канального уровня.

Разделенные на уровни протоколы стека TCP/IP спроектированы таким образом, что конкретный уровень хоста назначения получает именно тот объект, который был отправлен эквивалентным уровнем хоста источника. Каждый уровень стека одного хоста образует логическое соединение с одноименным уровнем стека другого хоста. При реализации физического соединения уровень передает свои данные интерфейсу уровня, расположенного выше или ниже в том же хосте. На рис. 2.2 показано, как осуществляется физическое и логическое соединение уровней. Вертикальные стрелки показывают физическое соединение в рамках одного хоста, а горизонтальные — логическое соединение между одноименными уровнями в различных хостах.

Следует обратить внимание на терминологию, традиционно используемую для обозначения информационных объектов, которые распространяются на интерфейсах между различными уровнями управления стека протоколов TCP/IP.

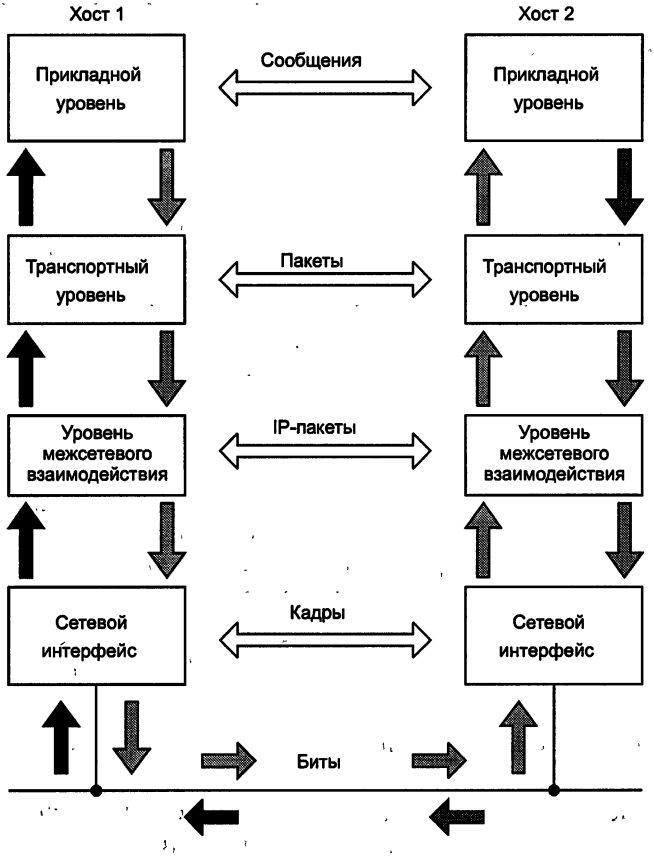


Рис. 2.2. Логические и физические соединения между уровнями стека TCP/IP

Приложение передает транспортному уровню сообщение (message), которое имеет соответствующие данному приложению размер и семантику. Транспортный уровень «разрезает» это сообщение (если оно достаточно велико) на пакеты (packets), которые передаются уровню межсетевого взаимодействия (т. е. протоколу IP). Протокол IP формирует свои IP-пакеты (еще говорят «IP-дейтаграммы») и затем упаковывает их в формат, приемлемый для данной физической среды передачи информации. Эти, уже аппаратно-зависимые, пакеты обычно называют кадрами (Frame).

Когда данные передаются от прикладного уровня к транспортному, затем к уровню межсетевого взаимодействия и далее через уровень сетевого интерфейса в сеть, каждый протокол выполняет соответствующую обработку и инкапсулирует результат этой обработки, присоединяя спереди свой заголовок. На рис. 2.3 показана схема процесса инкапсуляции передаваемых данных и формирования заголовков пакетов в стеке TCP/IP.

В системе, принимающей данный поток информации, эти заголовки последовательно удаляются по мере обработки данных и передачи их вверх по стеку. Такой подход обеспечивает необходимую гибкость в

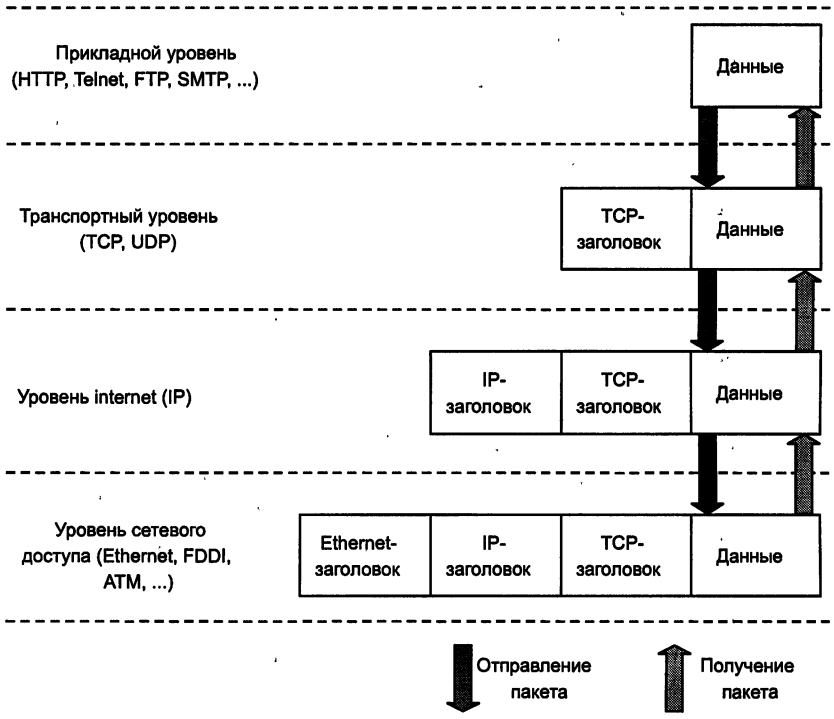


Рис. 2.3. Схема инкапсуляции данных в стеке протоколов TCP/IP

обработке передаваемых данных, поскольку верхним уровням вовсе не нужно касаться технологии, используемой на нижних уровнях. Например, если шифруются данные на уровне IP, уровень TCP и прикладной остаются неизменными.

Что касается безопасности протоколов TCP/IP, т. е. безопасности передачи данных в Интернете в целом, пользователям необходимо иметь в виду, что, если не принято специальных мер, все данные передаются протоколами TCP/IP в открытом виде. Это значит, что любой узел (и соответственно, его оператор), находящийся на пути следования данных от отправителя к получателю, может скопировать себе все передаваемые данные и использовать их в дальнейшем в своих целях. В равной мере данные могут быть искажены или уничтожены.

2.2. Анализ угроз сетевой безопасности

Для организации коммуникаций в неоднородной сетевой среде применяется набор протоколов TCP/IP, обеспечивая совместимость между компьютерами разных типов. Совместимость — одно из основных преимуществ TCP/IP, поэтому большинство компьютерных сетей поддерживает эти протоколы. Кроме того, протоколы TCP/IP предоставляют доступ к ресурсам глобальной сети Интернет.

Благодаря своей популярности TCP/IP стал стандартом де-факто для межсетевого взаимодействия. Однако повсеместное распространение стека протоколов TCP/IP обнажило и его слабые стороны. Создавая свое детище, архитекторы стека TCP/IP не видели причин особенно беспокоиться о защите сетей, строящихся на его основе. Поэтому в спецификациях ранних версий протокола IP отсутствовали требования безопасности, что привело к изначальной уязвимости реализации этого протокола.

2.2.1. Проблемы безопасности IP-сетей

Стремительный рост популярности интернет-технологий сопровождается ростом серьезных угроз разглашения персональных данных, критически важных корпоративных ресурсов, государственных тайн и т. д.

Характерные особенности сетевых атак

Каждый день хакеры и другие злоумышленники подвергают угрозам сетевые информационные ресурсы, пытаясь получить к ним доступ с помощью специальных атак. Эти атаки становятся все более изощренными по воздействию и несложными в исполнении. Этому способствуют два основных фактора.

Во-первых, это повсеместное проникновение Интернета. Сегодня к этой сети подключены миллионы компьютеров. Многие миллионы компьютеров будут подключены к Интернету в ближайшем будущем, поэтому вероятность доступа хакеров к уязвимым компьютерам и компьютерным сетям постоянно возрастает. Кроме того, широкое распространение Интернета позволяет хакерам обмениваться информацией в глобальном масштабе.

Во-вторых, это всеобщее распространение простых в использовании операционных систем и сред разработки. Этот фактор резко снижает требования к уровню знаний злоумышленника. Раньше от хакера требовались хорошие знания и навыки программирования, чтобы создавать и распространять вредоносные программы. Теперь, для того чтобы получить доступ к хакерскому средству, нужно просто знать IP-адрес нужного сайта, а для проведения атаки достаточно щелкнуть мышью.

Проблемы обеспечения информационной безопасности в корпоративных компьютерных сетях обусловлены угрозами безопасности для локальных рабочих станций, локальных сетей и из-за атак на корпоративные сети, имеющие выход в общедоступные сети передачи данных.

Сетевые атаки столь же разнообразны, как и системы, против которых они направлены. Некоторые атаки отличаются большой сложностью. Другие может осуществить обычный оператор, даже не предполагающий, какие последствия может иметь его деятельность.

Нарушитель, осуществляя атаку, обычно ставит перед собой следующие цели:

- нарушение конфиденциальности передаваемой информации;
- нарушение целостности и достоверности передаваемой информации;
- нарушение работоспособности системы в целом или отдельных ее частей.

С точки зрения безопасности распределенные системы характеризуются прежде всего наличием *удаленных атак*, поскольку компоненты распределенных систем обычно используют открытые каналы передачи данных и нарушитель может не только проводить пассивное прослушивание передаваемой информации, но и модифицировать передаваемый трафик (активное воздействие). И если активное воздействие на трафик может быть зафиксировано, то пассивное воздействие практически не поддается обнаружению. Но поскольку в ходе функционирования распределенных систем обмен служебной информацией между компонентами системы осуществляется тоже по открытым каналам передачи данных, то служебная информация становится таким же объектом атаки, как и данные пользователя.

Трудность выявления факта проведения удаленной атаки выводит этот вид неправомерных действий на первое место по степени опасности, поскольку необнаруживаемость препятствует своевременному реагированию на осуществленную угрозу, в результате чего у нарушителя увеличиваются шансы успешной реализации атаки.

Безопасность локальной сети по сравнению с безопасностью межсетевого взаимодействия отличается тем, что в этом случае на первое по значимости место выходят *нарушения зарегистрированных пользователей*, поскольку в основном каналы передачи данных локальной сети находятся на контролируемой территории, защита от несанкционированного подключения к которым реализуется административными методами.

На практике IP-сети уязвимы для ряда способов несанкционированного вторжения в процесс обмена данными. По мере развития компьютерных и сетевых технологий (например, с появлением мобильных Java-приложений и элементов ActiveX) список возможных типов сетевых атак на IP-сети постоянно расширяется [7].

Рассмотрим наиболее распространенные виды сетевых атак.

Подслушивание (Sniffing). По большей части данные по компьютерным сетям передаются в незащищенном формате (открытым текстом), что позволяет злоумышленнику, получившему доступ к линиям передачи данных в вашей сети, подслушивать или считывать трафик. Для подслушивания в компьютерных сетях используют сниффер. *Сниффер пакетов* представляет собой прикладную программу, которая перехватывает все сетевые пакеты, передаваемые через определенный домен.

В настоящее время снифферы работают в сетях на вполне законном основании. Они используются для диагностики неисправностей и анализа трафика. Однако ввиду того, что некоторые сетевые приложения

передают данные в текстовом формате (Telnet, FTP, SMTP, POP3 и т. д.); с помощью сниффера можно узнать полезную, а иногда и конфиденциальную информацию (например, имена пользователей и пароли).

Перехват пароля (Password Sniffing), передаваемого по сети в незашифрованной форме, путем «подслушивания» канала является разновидностью атаки подслушивания. Перехват имен и паролей создает большую опасность, так как пользователи часто применяют один и тот же логин и пароль для множества приложений и систем. Многие пользователи вообще имеют один пароль для доступа ко всем ресурсам и приложениям. Если приложение работает в режиме клиент/сервер, а аутентификационные данные передаются по сети в читаемом текстовом формате, эту информацию с большой вероятностью можно использовать для доступа к другим корпоративным или внешним ресурсам.

В самом худшем случае хакер получает доступ к пользовательскому ресурсу на системном уровне и с его помощью создает атрибуты нового пользователя, которые можно в любой момент применить для доступа в сеть и к ее ресурсам.

Предотвратить угрозу сниффинга пакетов можно с помощью следующих мер и средств: применение для аутентификации однократных паролей; установка аппаратных или программных средств, распознающих снифферы; применение криптографической защиты каналов связи.

Изменение данных. Злоумышленник, получивший возможность прочитать ваши данные, сможет сделать и следующий шаг — изменить их. Данные в пакете могут быть изменены, даже если злоумышленник ничего не знает ни об отправителе, ни о получателе. Даже если вы не нуждаетесь в строгой конфиденциальности всех передаваемых данных, наверняка вы не захотите, чтобы они были изменены по пути.

Анализ сетевого трафика. Целью атак подобного типа являются прослушивание каналов связи и анализ передаваемых данных и служебной информации с целью изучения топологии и архитектуры построения системы, получения критической пользовательской информации (например, паролей пользователей или номеров кредитных карт, передаваемых в открытом виде). Атакам данного типа подвержены такие протоколы, как FTP и Telnet, особенностью которых является то, что имя и пароль пользователя передаются в рамках этих протоколов в открытом виде.

Подмена доверенного субъекта. Бо льшаячасть сетей и операционных систем используют IP-адрес компьютера для того, чтобы определять, тот ли это адресат, который нужен. В некоторых случаях возможно некорректное присвоение IP-адреса (подмена IP-адреса отправителя другим адресом) — такой способ атаки называют *фальсификацией адреса*, или *IP-спуфингом* (*IP-spoofing*).

IP-спуфинг имеет место, когда злоумышленник, находящийся внутри корпорации или вне ее, выдает себя за законного пользователя. Злоумышленник может воспользоваться IP-адресом, находящимся в пределах диапазона санкционированных IP-адресов, или авторизованным

внешним адресом, которому разрешается доступ к определенным сетевым ресурсам. Злоумышленник может также использовать специальные программы, формирующие IP-пакеты таким образом, чтобы они выглядели как исходящие с разрешенных внутренних адресов корпоративной сети.

Атаки IP-спуфинга часто являются отправной точкой для других атак. Классическим примером является атака типа «отказ в обслуживании» (DoS), которая начинается с чужого адреса, скрывающего истинную личность хакера. Обычно IP-спуфинг ограничивается вставкой ложной информации или вредоносных команд в обычный поток данных, передаваемых между клиентским и серверным приложениями или по каналу связи между одноранговыми устройствами.

Угрозу спуфинга можно ослабить (но не устранить) с помощью следующих мер: правильная настройка управления доступом из внешней сети; пресечение попыток спуфинга чужих сетей пользователями своей сети.

Следует иметь в виду, что IP-спуфинг может быть осуществлен при условии, что аутентификация пользователей производится на базе IP-адресов, поэтому введение дополнительных методов аутентификации пользователей (на основе одноразовых паролей или других методов криптографии) позволяет предотвратить атаки IP-спуфинга.

Посредничество. Атака типа «посредничество» подразумевает активное подслушивание, перехват и управление передаваемыми данными невидимым промежуточным узлом. Когда компьютеры взаимодействуют на низких сетевых уровнях, они не всегда могут определить, с кем именно они обмениваются данными.

Посредничество в обмене незашифрованными ключами (атака Man-in-the-Middle — «человек-в-середине»). Для проведения атаки «человек-в-середине» злоумышленнику нужен доступ к пакетам, передаваемым по сети. Такой доступ ко всем пакетам, передаваемым от провайдера ISP в любую другую сеть, может, например, получить сотрудник этого провайдера. Для атак этого типа часто используются снифферы пакетов, транспортные протоколы и протоколы маршрутизации.

В более общем случае атаки «человек-в-середине» проводятся с целью кражи информации, перехвата текущей сессии и получения доступа к частным сетевым ресурсам, для анализа трафика и получения информации о сети и ее пользователях, для проведения атак типа DoS, искажения передаваемых данных и ввода несанкционированной информации в сетевые сессии.

Эффективно бороться с атаками типа «человек-в-середине» можно только с помощью криптографии. Для противодействия атакам этого типа используется *инфраструктура управления открытыми ключами PKI* (Public Key Infrastructure).

Перехват сеанса (Session Hijacking). По окончании начальной процедуры аутентификации соединение, установленное законным пользователем, например, с почтовым сервером, переключается злоумышленником на новый хост, а исходному серверу выдается команда разорвать

соединение. В результате «собеседник» законного пользователя оказывается незаметно подмененным.

После получения доступа к сети у атакующего злоумышленника появляются большие возможности:

- он может посылать некорректные данные приложениям и сетевым службам, что приводит к их аварийному завершению или неправильному функционированию;
- он может также наводнить компьютер или всю сеть трафиком, пока не произойдет останов системы в связи с перегрузкой;
- наконец, атакующий может блокировать трафик, что приведет к потере доступа авторизованных пользователей к сетевым ресурсам.

Отказ в обслуживании — DoS (Denial of Service). Эта атака отличается от атак других типов. Она не нацелена на получение доступа к вашей сети или на получение из этой сети какой-либо информации. Атака DoS делает сеть организации недоступной для обычного использования за счет превышения допустимых пределов функционирования сети, операционной системы или приложения. По существу, эта атака лишает обычных пользователей доступа к ресурсам или компьютерам сети организации.

Большинство атак DoS опирается на общие слабости системной архитектуры. В случае использования некоторых серверных приложений (таких, как веб- или FTP-сервер) атаки DoS могут заключаться в том, чтобы занять все соединения, доступные для этих приложений, и держать их в занятом состоянии, не допуская обслуживания обычных пользователей. В ходе атак DoS могут использоваться обычные интернет-протоколы, такие как TCP и ICMP (Internet Control Message Protocol).

Атаки DoS трудно предотвратить, так как для этого требуется координация действий с провайдером. Если трафик, предназначенный для переполнения вашей сети, не остановить у провайдера, то на входе в сеть вы это сделать уже не сможете, потому что вся полоса пропускания будет занята.

Если атака этого типа проводится одновременно через множество устройств, мы говорим о *распределенной атаке отказа в обслуживании DDoS (Distributed DoS).*

Простота реализации атак DoS и огромный вред, причиняемый ими организациям и пользователям, привлекают к этим атакам пристальное внимание администраторов сетевой безопасности.

Парольные атаки. Целью этих атак является завладение паролем и логином законного пользователя. Злоумышленники могут проводить парольные атаки, используя такие методы, как:

- подмена IP-адреса (IP-спуфинг);
- подслушивание (сниффинг);
- простой перебор.

IP-спуфинг и сниффинг пакетов были рассмотрены выше. Эти методы позволяют завладеть паролем и логином пользователя, если они передаются открытым текстом по незащищенному каналу.

Часто хакеры пытаются подобрать пароль и логин, используя для этого многочисленные попытки доступа. Такой подход носит название *«атака полного перебора» (Brute Force Attack)*. Для этой атаки используется специальная программа, которая пытается получить доступ к ресурсу общего пользования (например, к серверу). Если в результате злоумышленнику удается подобрать пароль, он получает доступ к ресурсам на правах обычного пользователя. Если этот пользователь имеет значительные привилегии доступа, злоумышленник может создать для себя «проход» для будущего доступа, который будет действовать, даже если пользователь изменит свои пароль и логин.

Средства перехвата, подбора и взлома паролей в настоящее время считаются практически легальными и официально выпускаются достаточно большим числом компаний. Они позиционируются как программы для аудита безопасности и восстановления забытых паролей, и их можно на законных основаниях приобрести у разработчиков.

Парольных атак можно избежать, если не пользоваться паролями в текстовой форме. Использование одноразовых паролей и криптографической аутентификации могут практически свести на нет угрозу таких атак. К сожалению, не все приложения, хосты и устройства поддерживают указанные методы аутентификации.

При использовании обычных паролей необходимо придумать такой пароль, который было бы трудно подобрать. Минимальная длина пароля должна быть не менее восьми символов. Пароль должен включать символы верхнего регистра, цифры и специальные символы (#, $, &, % и т. д.).

Угадывание ключа. Криптографический ключ представляет собой код или число, необходимое для расшифровки защищенной информации. Хотя узнать ключ доступа трудно и требует больших затрат ресурсов, тем не менее это возможно. В частности, для определения значения ключа может быть использована специальная программа, реализующая метод полного перебора. Ключ, к которому получает доступ атакующий, называется скомпрометированным. Атакующий использует скомпрометированный ключ для получения доступа к защищенным передаваемым данным без ведома отправителя и получателя. Ключ дает возможность расшифровывать и изменять данные.

Атаки на уровне приложений. Эти атаки могут проводиться несколькими способами. Самый распространенный из них состоит в использовании известных слабостей серверного программного обеспечения (FTP, HTTP, веб-сервера).

Главная проблема с атаками на уровне приложений состоит в том, что они часто пользуются портами, которым разрешен проход через межсетевой экран.

Сведения об атаках на уровне приложений широко публикуются, чтобы дать возможность администраторам устранить проблему с помощью коррекционных модулей (патчей). К сожалению, многие хакеры также имеют доступ к этим сведениям, что позволяет им учиться.

Невозможно полностью исключить атаки на уровне приложений. Хакеры постоянно открывают и публикуют на своих сайтах в Интернете все новые уязвимые места прикладных программ.

Здесь важно осуществлять хорошее системное администрирование. Чтобы снизить уязвимость от атак этого типа, можно предпринять следующие меры:

- анализировать лог-файлы операционных систем и сетевые лог-файлы с помощью специальных аналитических приложений;
- отслеживать данные CERT о слабых местах прикладных программ;
- пользоваться самыми свежими версиями операционных систем и приложений и самыми последними коррекционными модулями (патчами);
- использовать системы распознавания атак IDS (Intrusion Detection Systems).

Сетевая разведка — это сбор информации о сети с помощью общедоступных данных и приложений. При подготовке атаки против какой-либо сети хакер, как правило, пытается получить о ней как можно больше информации.

Сетевая разведка проводится в форме запросов DNS, эхо-тестирования (Ping Sweep) и сканирования портов. Запросы DNS помогают понять, кто владеет тем или иным доменом и какие адреса этому домену присвоены. Эхо-тестирование адресов, раскрытых с помощью DNS, позволяет увидеть, какие хосты реально работают в данной среде. Получив список хостов, хакер использует средства сканирования портов, чтобы составить полный список услуг, поддерживаемых этими хостами. В результате добывается информация, которую можно использовать для взлома.

Полностью избавиться от сетевой разведки невозможно. Если, к примеру, отключить эхо ICMP и эхо-ответ на периферийных маршрутизаторах, вы избавитесь от эхо-тестирования, но потеряете данные, необходимые для диагностики сетевых сбоев. Кроме того, сканировать порты можно и без предварительного эхо-тестирования. Просто это займет больше времени, так как сканировать придется и несуществующие IP-адреса.

Системы IDS на уровне сети и хостов обычно хорошо справляются с задачей уведомления администратора о ведущейся сетевой разведке, что позволяет лучше подготовиться к предстоящей атаке и оповестить провайдера (ISP), в сети которого установлена система, проявляющая чрезмерное любопытство.

Злоупотребление доверием. Данный тип действий не является атакой в полном смысле этого слова. Он представляет собой злонамеренное использование отношений доверия, существующих в сети. Типичным примером такого злоупотребления является ситуация в периферийной части корпоративной сети. В этом сегменте обычно располагаются серверы DNS, SMTP и HTTP. Поскольку все они принадлежат к одному и тому же сегменту, взлом одного из них приводит

к взлому и всех остальных, так как эти серверы доверяют другим системам своей сети.

Риск злоупотребления доверием можно снизить за счет более жесткого контроля уровней доверия в пределах своей сети. Системы, расположенные с внешней стороны межсетевого экрана, никогда не должны пользоваться абсолютным доверием со стороны систем, защищенных межсетевым экраном.

Отношения доверия должны ограничиваться определенными протоколами и, по возможности, аутентифицироваться не только по IP-адресам, но и по другим параметрам.

Перечисленные атаки на IP-сети возможны в силу ряда причин:

- использование общедоступных каналов передачи данных. Важнейшие данные передаются по сети в незашифрованном виде;
- уязвимости в процедурах идентификации, реализованных в стеке TCP/IP. Идентифицирующая информация на уровне IP передается в открытом виде;
- отсутствие в базовой версии стека протоколов TCP/IP механизмов, обеспечивающих конфиденциальность и целостность передаваемых сообщений;
- аутентификация отправителя осуществляется по его IP-адресу. Процедура аутентификации выполняется только на стадии установления соединения, а в дальнейшем подлинность принимаемых пакетов не проверяется;
- отсутствие возможности контроля за маршрутом прохождения сообщений в сети Интернет, что делает удаленные сетевые атаки практически безнаказанными.

Криминализация атак на компьютерные сети и системы. В последние годы растет криминализация атак на информационные системы. Киберпреступность изменяется не только количественно, но и качественно. Школьников и студентов, которые раньше писали большинство вирусов и занимались хакингом из любопытства и тщеславия, сейчас заменяют «серьезные люди», строящие на реализации угроз информационной безопасности свой бизнес. Вместо хаотичного распространения вредоносных программ они организуют направленные комплексные атаки на системы организаций-жертв с четкой целью завладения конфиденциальной информацией или хищения денежных средств в электронных расчетных системах. Это также влияет на статистику реализованных угроз и постепенное наращивание доли шпионящих и троянских программ, а также фишинга.

Компьютерные преступления перемещаются в область организованной преступности и получают все более четкую ориентацию на получение доходов в результате их совершения. Растет число инцидентов, связанных с нелегальным получением доступа к конфиденциальной информации, вымогательством под угрозой организации атаки на компьютерную систему, подкупом сотрудников атакуемой организации, заказными атаками «отказ в обслуживании» коммерческих интернет-порталов. Онлайн-криминал незаметно превратился в организованный и

очень живучий бизнес с инновациями, инвестициями и транснациональной структурой.

Переход компьютерных преступлений «на деловые рельсы» и повышение организованности атак на информационные системы вызывает серьезный рост опасности их последствий для атакуемых организаций.

Поэтому эксперты по информационной безопасности настойчиво рекомендуют компаниям использовать комплексные системы защиты информации, выявления угроз, блокирования известных и неизвестных вредоносных программ, а также мониторинга работы пользователей и предотвращения инсайдерских атак.

2.2.2. Угрозы и уязвимости беспроводных сетей

При построении беспроводных сетей одной из наиболее острых проблем является обеспечение их безопасности. Если в обычных сетях информация передается по проводам, то радиоволны, используемые для беспроводных решений, достаточно легко перехватить при наличии соответствующего оборудования. Принцип действия беспроводной сети приводит к возникновению большого количества возможных уязвимостей для атак и проникновений.

Оборудование беспроводных локальных сетей WLAN (Wireless Local Area Network) включает в себя точки беспроводного доступа и рабочие станции для каждого абонента.

Точки доступа AP (Access Point) выполняют роль концентраторов, обеспечивающих связь между абонентами и между собой, а также функцию мостов, осуществляющих связь с кабельной локальной сетью и с Интернетом. Каждая точка доступа может обслуживать несколько абонентов. Несколько близко расположенных точек доступа образуют зону доступа Wi-Fi, в пределах которой все абоненты, снабженные беспроводными адаптерами, получают доступ к сети. Такие зоны доступа создаются в местах массового скопления людей: в аэропортах, студенческих городках, библиотеках, магазинах, бизнес-центрах и т. д.

У точки доступа есть идентификатор набора сервисов SSID (Service Set Identifier). SSID — это 32-битная строка, используемая в качестве имени беспроводной сети, с которой ассоциируются все узлы. Идентификатор SSID необходим для подключения рабочей станции к сети. Чтобы связать рабочую станцию с точкой доступа, обе системы должны иметь один и тот же SSID. Если рабочая станция не имеет нужного SSID, то она не сможет связаться с точкой доступа и соединиться с сетью.

Главное отличие между проводными и беспроводными сетями связано с наличием неконтролируемой области между конечными точками беспроводной сети. Это позволяет атакующим, находящимся в непосредственной близости от беспроводных структур, производить целый ряд нападений, которые невозможны в проводном мире.

При использовании беспроводного доступа к локальной сети угрозы безопасности существенно возрастают (рис. 2.4).

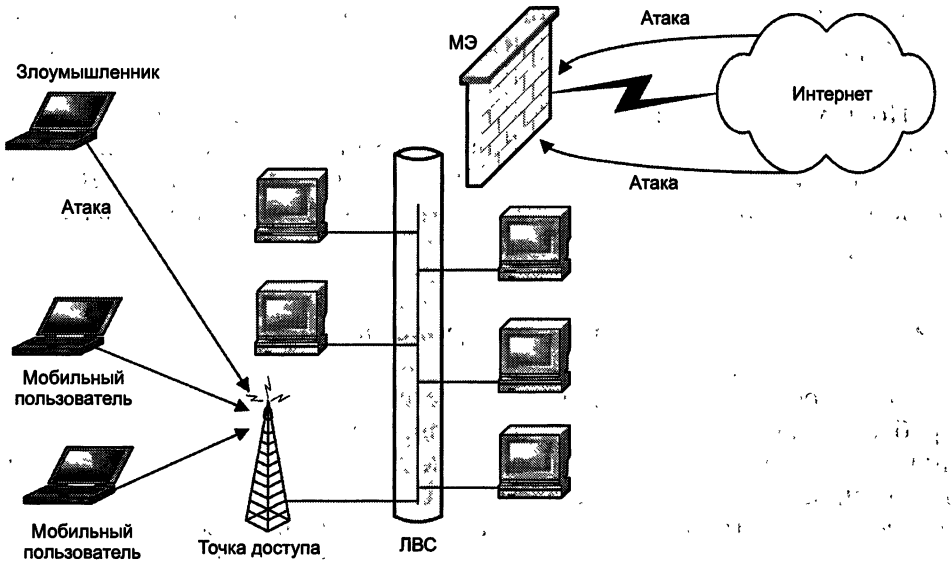


Рис. 2.4. Угрозы при беспроводном доступе к локальной сети

Перечислим основные уязвимости и угрозы беспроводных сетей.

Вещание радиомаяка. Точка доступа включает с определенной частотой широковещательный радиомаяк, чтобы оповещать окрестные беспроводные узлы о своем присутствии. Эти широковещательные сигналы содержат основную информацию о точке беспроводного доступа, включая, как правило, SSID, и приглашают зарегистрироваться беспроводные узлы в данной области. Любая рабочая станция, находящаяся в режиме ожидания, может получить SSID и добавить себя в соответствующую сеть. Вещание радиомаяка является врожденной патологией беспроводных сетей. Многие модели позволяют отключать содержащую SSID часть этого вещания, чтобы несколько затруднить беспроводное подслушивание, но SSID тем не менее посылается при подключении, поэтому все равно существует небольшое окно уязвимости.

Обнаружение WLAN. Для обнаружения беспроводных сетей WLAN используется, например, утилита NetStumber совместно со спутниковым навигатором глобальной системы позиционирования GPS. Данная утилита идентифицирует SSID сети WLAN, а также определяет, используется ли в ней система шифрования WEP. Применение внешней антенны на портативном компьютере делает возможным обнаружение сетей WLAN во время обхода нужного района или поездки по городу. Надежным методом обнаружения WLAN является обследование офисного здания с переносным компьютером в руках.

Подслушивание. Подслушивание ведут для сбора информации о сети, которую предполагается атаковать впоследствии. Перехватчик мо-

жет использовать добытые данные для того, чтобы получить доступ к сетевым ресурсам. Оборудование, используемое для подслушивания в сети, может быть не сложнее того, которое применяется для обычного доступа к этой сети. Беспроводные сети по своей природе позволяют соединять с физической сетью компьютеры, находящиеся на некотором расстоянии от нее, как если бы эти компьютеры находились непосредственно в сети. Это позволяет подключиться к беспроводной сети, располагающейся в здании, человеку, сидящему в машине на стоянке рядом с ним. Атаку посредством пассивного прослушивания практически невозможно обнаружить.

Ложные точки доступа в сеть. Опытный атакующий может организовать ложную точку доступа с имитацией сетевых ресурсов. Абоненты, ничего не подозревая, обращаются к этой ложной точке доступа и сообщают ей свои важные реквизиты, например аутентификационную информацию. Этот тип атак иногда применяют в сочетании с прямым глушением, чтобы заглушить истинную точку доступа в сеть.

Отказ в обслуживании. Полную парализацию сети может вызвать атака типа «отказ в обслуживании» (DoS). Цель любой атаки отказа в обслуживании состоит в создании помехи при доступе пользователя к сетевым ресурсам. Беспроводные системы особенно восприимчивы к таким атакам. Физический уровень в беспроводной сети — абстрактное пространство вокруг точки доступа. Злоумышленник может включить устройство, заполняющее весь спектр на рабочей частоте помехами и нелегальным трафиком, — такая задача не вызывает особых трудностей. Сам факт проведения DoS-атаки на физическом уровне в беспроводной сети трудно доказать.

Атаки типа «человек-в-середине». Атаки типа «человек-в-середине» выполняются на беспроводных сетях гораздо проще, чем на проводных, так как к проводной сети требуется реализовать определенный вид доступа. Обычно атаки «человек-в-середине» используются для нарушения конфиденциальности и целостности сеанса связи. Атаки «человек-в-середине» более сложны, чем большинство других атак: для их проведения требуется подробная информация о сети. Злоумышленник обычно подменяет идентификацию одного из сетевых ресурсов. Злоумышленник использует возможность прослушивания и нелегального захвата потока данных с целью изменения его содержимого, необходимого для удовлетворения некоторых своих целей, например для спуфинга IP-адресов, изменения MAC-адреса для имитирования другого хоста и т. д.

Анонимный доступ в Интернет. Незащищенные беспроводные ЛВС (локальные вычислительные сети) обеспечивают хакерам наилучший анонимный доступ для атак через Интернет. Хакеры могут использовать незащищенную беспроводную ЛВС организации для выхода через нее в Интернет, где они будут осуществлять противоправные действия, не оставляя при этом своих следов. Организация с незащищенной ЛВС формально становится источником атакующего трафика, нацеленного на другую компьютерную систему, что связано с потенциальным рис-

ком правовой ответственности за причиненный ущерб жертве атаки хакеров.

Атаки, используемые хакерами для взлома беспроводных сетей, не ограничиваются описанными выше.

2.3. Обеспечение информационной безопасности сетей

2.3.1. Способы обеспечения информационной безопасности

Существует два подхода к проблеме обеспечения безопасности компьютерных систем и сетей: фрагментарный и комплексный [7].

Фрагментарный подход направлен на противодействие четко определенным угрозам в заданных условиях. В качестве примеров реализации такого подхода можно указать отдельные средства управления доступом, автономные средства шифрования, специализированные антивирусные программы и т. п.

Достоинством такого подхода является высокая избирательность к конкретной угрозе. Существенным недостатком данного подхода является отсутствие единой защищенной среды обработки информации. Фрагментарные меры защиты информации обеспечивают защиту конкретных объектов КС только от конкретной угрозы. Даже небольшое видоизменение угрозы ведет к потере эффективности защиты.

Комплексный подход ориентирован на создание защищенной среды обработки информации в КС, объединяющей в единый комплекс разнородные меры противодействия угрозам. Организация защищенной среды обработки информации позволяет гарантировать определенный уровень безопасности КС, что является несомненным достоинством комплексного подхода. К недостаткам этого подхода относятся: ограничения на свободу действий пользователей КС, чувствительность к ошибкам установки и настройки средств защиты, сложность управления.

Комплексный подход применяют для защиты КС крупных организаций или небольших КС, выполняющих ответственные задачи либо обрабатывающих особо важную информацию. Нарушение безопасности информации в КС крупных организаций может нанести огромный материальный ущерб как самим организациям, так и их клиентам. Поэтому такие организации вынуждены уделять особое внимание гарантиям безопасности и реализовывать комплексную защиту. Комплексного подхода придерживаются большинство государственных и крупных коммерческих предприятий и учреждений. Этот подход нашел свое отражение в различных стандартах.

Комплексный подход к проблеме обеспечения безопасности основан на разработанной для конкретной КС политике безопасности. Политика безопасности регламентирует эффективную работу средств за-

щиты КС. Она охватывает все особенности процесса обработки информации, определяя поведение системы в различных ситуациях. Надежная система безопасности сети не может быть создана без эффективной политики сетевой безопасности. Построение и применение политик безопасности подробно рассматривается в главе 3.

Для защиты интересов субъектов информационных отношений необходимо сочетать меры следующих уровней:

- законодательного (стандарты, законы, нормативные акты и т. п.);
- административно-организационного (действия общего характера, предпринимаемые руководством организации, и конкретные меры безопасности, касающиеся людей);
- программно-технического (конкретные технические меры).

Меры законодательного уровня очень важны для обеспечения информационной безопасности. К этому уровню можно отнести весь комплекс мер, направленных на создание и поддержание в обществе негативного (в том числе карательного) отношения к нарушениям и нарушителям информационной безопасности. Большинство людей не совершают противоправных действий потому, что это осуждается и/или наказывается обществом, и потому, что так поступать не принято.

Информационная безопасность — это новая область деятельности, здесь важно не только запрещать и наказывать, но и научить, разъяснить, помочь. Общество должно осознать важность этой области, понять основные пути решения соответствующих проблем. Государство может сделать это оптимальным образом. Здесь не нужно больших материальных затрат, требуются интеллектуальные вложения.

Меры административно-организационного уровня. Администрация организации должна сознавать необходимость поддержания режима безопасности и выделения на эти цели соответствующих ресурсов. Основой мер защиты административно-организационного уровня является политика безопасности и комплекс организационных мер. Под политикой безопасности понимается совокупность документированных управленческих решений, направленных на защиту информации и ассоциированных с ней ресурсов организации.

К комплексу организационных мер относятся меры безопасности, реализуемые людьми. Можно выделить следующие группы организационных мер:

- управление персоналом;
- физическая защита;
- поддержание работоспособности;
- реагирование на нарушения режима безопасности;
- планирование восстановительных работ.

Для каждой группы в каждой организации должен существовать набор регламентов, определяющих действия персонала.

Для поддержания режима информационной безопасности особенно важны меры программно-технического уровня, поскольку основная угроза компьютерным системам исходит от них самих: сбои оборудова-

ния, ошибки программного обеспечения, промахи пользователей и администраторов и т. п.

Меры и средства программно-технического уровня. В рамках современных информационных систем должны быть доступны по крайней мере следующие механизмы безопасности:

- идентификация и проверка подлинности пользователей;
- управление доступом;
- протоколирование и аудит;
- криптография;
- экранирование;
- обеспечение высокой доступности.

Необходимость применения стандартов. Информационные системы компаний почти всегда построены на основе программных и аппаратных продуктов различных производителей. Дело в том, что на данный момент нет ни одной компании-разработчика, которая предоставила бы потребителю полный перечень средств (от аппаратных до программных) для построения современной ИС. Чтобы обеспечить в разнородной ИС надежную защиту информации, требуются специалисты высокой квалификации, которые будут отвечать за безопасность каждого компонента ИС: правильно их настраивать, постоянно отслеживать происходящие изменения, контролировать работу пользователей. Очевидно, что чем разнороднее информационная система, тем сложнее обеспечить ее безопасность. Изобилие в корпоративных сетях и системах устройств защиты, межсетевых экранов, шлюзов и VPN, а также растущий спрос на доступ к корпоративным данным со стороны сотрудников, партнеров и заказчиков приводят к созданию сложной среды защиты, трудной для управления, а иногда и несовместимой.

Интероперабельность продуктов защиты является важным требованием для большинства корпоративных информационных систем. Для большинства гетерогенных сред важно обеспечить согласованное взаимодействие с продуктами других производителей. Принятое организацией решение безопасности должно гарантировать защиту на всех платформах в рамках этой организации. Поэтому вполне очевидна потребность в применении единого набора стандартов поставщиками средств защиты, компаниями — системными интеграторами и организациями, выступающими в качестве заказчиков систем безопасности для своих корпоративных сетей и систем.

Стандарты образуют понятийный базис, на котором строятся все работы по обеспечению информационной безопасности, и определяют критерии управления безопасностью. Стандарты являются необходимой базой, обеспечивающей совместимость продуктов разных производителей, что чрезвычайно важно при создании систем сетевой безопасности в гетерогенных средах. Международные и отечественные стандарты информационной безопасности рассматриваются в главе 16.

Комплексный подход к решению проблемы обеспечения безопасности, рациональное сочетание законодательных, административно-орга-

низационных и программно-технических мер и обязательное следование промышленным, национальным и международным стандартам являются тем фундаментом, на котором строится вся система защиты корпоративных сетей.

2.3.2. Пути решения проблем защиты информации в сетях

Для поиска решений проблем информационной безопасности при работе в сети Интернет был создан независимый консорциум ISTF (Internet Security Task Force) — общественная организация, состоящая из представителей и экспертов компаний — поставщиков средств информационной безопасности, электронного бизнеса и провайдеров интернет-инфраструктуры. Цель этого консорциума — разработка технических, организационных и операционных руководств по безопасности деятельности в Интернете.

Консорциум ISTF выделил двенадцать областей информационной безопасности, на которых в первую очередь должны сконцентрировать свое внимание создатели электронного бизнеса, чтобы обеспечить его работоспособность. Этот список, в частности, включает следующие пункты:

- аутентификация (механизм объективного подтверждения идентифицирующей информации);
- право на частную, персональную информацию (обеспечение конфиденциальности информации);
- определение событий безопасности (Security Events);
- защита корпоративного периметра;
- определение атак;
- контроль за потенциально опасным содержимым (Malicious Content);
- контроль доступа;
- администрирование;
- реакция на события (Incident Response).

Рекомендации ISTF предназначены для существующих или вновь образуемых компаний электронной коммерции и электронного бизнеса. Эти рекомендации помогают определить потенциальные бреши в их компьютерных сетях, которые, если не обратить на них должного внимания, могут использоваться взломщиками. Это может привести к атакам на систему электронной коммерции, потрясениям и даже к крушению электронного бизнеса. Консорциум ISTF настоятельно рекомендовал воспользоваться его наработками еще до начала организации компании, намеревающейся заняться электронной коммерцией и бизнесом.

Реализация рекомендаций консорциума ISTF означает, что защита информации в системе электронного бизнеса должна быть комплексной.

Для комплексной защиты от угроз и гарантии экономически выгодного и безопасного использования коммуникационных ресурсов для электронного бизнеса необходимо решить следующие задачи:

- проанализировать угрозы безопасности для системы электронного бизнеса;
- разработать политику информационной безопасности;
- защитить внешние каналы передачи информации, обеспечив конфиденциальность, целостность и подлинность передаваемой по ним информации;
- гарантировать возможность безопасного доступа к открытым ресурсам внешних сетей и Интернета, а также общения с пользователями этих сетей;
- защитить отдельные наиболее коммерчески значимые информационные системы независимо от используемых ими каналов передачи данных;
- предоставить защищенный удаленный доступ персонала к информационным ресурсам корпоративной сети;
- обеспечить надежное централизованное управление средствами сетевой защиты.

Согласно рекомендациям ISTF и классификации «рубежей обороны» Hurwitz Group, первым и важнейшим этапом разработки системы информационной безопасности электронного бизнеса являются механизмы управления доступом к сетям общего пользования и из них, а также механизмы безопасных коммуникаций, реализуемые межсетевыми экранами и продуктами частных защищенных виртуальных сетей (VPN).

Сопровождая их средствами интеграции и управления всей ключевой информацией системы защиты (PKI — инфраструктура открытых ключей), можно получить целостную, централизованно управляемую систему информационной безопасности.

Следующий рубеж включает в себя интегрируемые в общую структуру средства контроля доступа пользователей в систему вместе с системой однократного входа и авторизации (Single Sign-On).

Антивирусная защита, средства аудита и предотвращения атак, по существу, завершают создание интегрированной целостной системы безопасности, если речь не идет о работе с конфиденциальными данными. В этом случае потребуются также средства криптографической защиты данных и электронно-цифровой подписи.

Для реализации основных функциональных компонентов системы безопасности для электронного бизнеса применяются различные методы и средства защиты информации:

- защищенные коммуникационные протоколы;
- средства криптографии;
- механизмы аутентификации и авторизации;
- средства контроля доступа к рабочим местам сети и из сетей общего пользования;
- средства борьбы с вредоносными программами и спамом;

- программы обнаружения и предотвращения атак;
- средства централизованного управления контролем доступа пользователей, а также безопасного обмена пакетами данных и сообщениями любых приложений по открытым IP-сетям.

Применение комплекса средств защиты на всех уровнях корпоративной системы позволяет построить эффективную и надежную систему обеспечения информационной безопасности.

Перечисленные выше методы и средства защиты информации подробно рассматриваются в последующих главах книги.

Вопросы для самоконтроля

1. Опишите основные возможности, предоставляемые сетью Интернет для построения корпоративных сетей.
2. Что такое стандартная модель взаимодействия открытых систем ISO/OSI?
3. Назовите семь уровней взаимодействия в модели ISO/OSI и укажите, какие функции должен выполнять каждый из них.
4. Что представляет собой стек коммуникационных протоколов ISO/OSI? Укажите различия между моделью взаимодействия открытых систем ISO/OSI и стеком протоколов ISO/OSI.
5. Сформулируйте структуру и функциональность стека протоколов TCP/IP.
6. Назовите и охарактеризуйте наиболее распространенные виды сетевых атак.
7. Опишите атаку «человек-в-середине». Какие средства позволяют эффективно бороться с атаками такого типа?
8. Опишите атаку отказа в обслуживании и распределенную атаку отказа в обслуживании.
9. Опишите особенности фишинга и фарминга. Укажите меры противодействия этим атакам.
10. Каковы источники нарушений безопасности проводных корпоративных сетей?
11. Назовите основные уязвимости и угрозы беспроводных сетей.
12. Какие методы и средства защиты информации применяются для реализации основных функциональных компонентов системы безопасности КИС?

Глава 3
ПОЛИТИКА БЕЗОПАСНОСТИ

Под *политикой безопасности* организации понимают совокупность документированных управленческих решений, направленных на защиту информации и ассоциированных с ней ресурсов. Политика безопасности является тем средством, с помощью которого реализуется деятельность в компьютерной информационной системе организации. Вообще политики безопасности определяются используемой компьютерной средой и отражают специфические потребности организации.

Обычно корпоративная информационная система представляет собой сложный комплекс разнородного, иногда плохо согласующегося между собой аппаратного и программного обеспечения: компьютеров, операционных систем, сетевых средств, СУБД, разнообразных приложений. Все эти компоненты обычно обладают собственными средствами защиты, которые нужно согласовать между собой. Поэтому очень важна эффективная политика безопасности в качестве согласованной платформы по обеспечению безопасности корпоративной системы. По мере роста компьютерной системы и интеграции ее в глобальную сеть необходимо обеспечить отсутствие в системе слабых мест, поскольку все усилия по защите информации могут быть обесценены лишь одной оплошностью.

Можно построить такую политику безопасности, которая будет устанавливать, кто имеет доступ к конкретным активам и приложениям, какие роли и обязанности будут иметь конкретные лица, а также предусмотреть процедуры безопасности, которые четко предписывают, как должны выполняться конкретные задачи безопасности. Индивидуальные особенности работы сотрудника могут потребовать доступа к информации, которая не должна быть доступна другим работникам. Например, менеджер по персоналу может иметь доступ к частной информации любого сотрудника, в то время как специалист по отчетности может иметь доступ только к финансовым данным этих сотрудников. А рядовой сотрудник будет иметь доступ только к своей собственной персональной информации.

Политика безопасности определяет позицию организации по рациональному использованию компьютеров и сети, а также процедуры по предотвращению и реагированию на инциденты безопасности. В большой корпоративной системе может применяться широкий диапазон разных политик от бизнес-политик до специфичных правил доступа к наборам данных. Эти политики полностью определяются конкретными потребностями организации.

3.1. Основные понятия политики безопасности

Политика безопасности определяет стратегию управления в области информационной безопасности, а также ту меру внимания и количество ресурсов, которые считает целесообразным выделить руководство.

Политика безопасности строится на основе анализа рисков, которые признаются реальными для информационной системы организации. Когда проведен анализ рисков и определена стратегия защиты, составляется программа, реализация которой должна обеспечить информационную безопасность. Под эту программу выделяются ресурсы, назначаются ответственные, определяется порядок контроля выполнения программы и т. п.

Для того чтобы ознакомиться с основными понятиями политик безопасности, рассмотрим в качестве конкретного примера гипотетическую локальную сеть, принадлежащую некоторой организации, и ассоциированную с ней политику безопасности [6, 67].

Политика безопасности организации должна иметь структуру краткого, легко понимаемого документа высокоуровневой политики, поддерживаемого рядом более конкретных документов специализированных политик и процедур безопасности.

Высокоуровневая политика безопасности должна периодически пересматриваться, чтобы гарантировать, что она учитывает текущие потребности организации. Этот документ составляют таким образом, чтобы политика была относительно независимой от конкретных технологий. В таком случае этот документ политики не потребуется изменять слишком часто.

Политика безопасности обычно оформляется в виде документа, включающего такие разделы, как описание проблемы, область применения, позиция организации, распределение ролей и обязанностей, санкции и др.

Описание проблемы. Информация, циркулирующая в рамках локальной сети, является критически важной. Локальная сеть позволяет пользователям совместно использовать программы и данные, что увеличивает угрозу безопасности. Поэтому каждый из компьютеров, входящих в сеть, нуждается в более сильной защите. Эти повышенные меры безопасности и являются темой данного документа. Документ преследует следующие цели: продемонстрировать сотрудникам организации важность защиты сетевой среды, описать их роль в обеспечении безопасности, а также распределить конкретные обязанности по защите информации, циркулирующей в сети.

Область применения. В сферу действия данной политики попадают все аппаратные, программные и информационные ресурсы, входящие в локальную сеть предприятия. Политика ориентирована также на людей, работающих с сетью, в том числе на пользователей, субподрядчиков и поставщиков.

Позиция организации. Целью организации является обеспечение целостности, доступности и конфиденциальности данных, а также их полноты и актуальности. Более частными целями являются:

- обеспечение уровня безопасности, соответствующего нормативным документам;
- следование экономической целесообразности в выборе защитных мер (расходы на защиту не должны превосходить предполагаемый ущерб от нарушения информационной безопасности);
- обеспечение безопасности в каждой функциональной области локальной сети;
- обеспечение подотчетности всех действий пользователей с информацией и ресурсами;
- обеспечение анализа регистрационной информации;
- предоставление пользователям достаточной информации для сознательного поддержания режима безопасности;
- выработка планов восстановления после аварий и иных критических ситуаций для всех функциональных областей с целью обеспечения непрерывности работы сети;
- обеспечение соответствия с имеющимися законами и общеорганизационной политикой безопасности.

Распределение ролей и обязанностей. За реализацию сформулированных выше целей отвечают соответствующие должностные лица и пользователи сети.

Руководители подразделений отвечают за доведение положений политики безопасности до пользователей и за контакты с ними.

Администраторы локальной сети обеспечивают непрерывное функционирование сети и отвечают за реализацию технических мер, необходимых для проведения в жизнь политики безопасности.

Администраторы сервисов отвечают за конкретные сервисы и, в частности, за то, чтобы защита была построена в соответствии с общей политикой безопасности.

Пользователи обязаны работать с локальной сетью в соответствии с политикой безопасности, подчиняться распоряжениям лиц, отвечающих за отдельные аспекты безопасности, ставить в известность руководство обо всех подозрительных ситуациях.

Ниже приведены более подробные сведения о ролях и обязанностях должностных лиц и пользователей сети.

Санкции. Нарушение политики безопасности может подвергнуть локальную сеть и циркулирующую в ней информацию недопустимому риску. Случаи нарушения безопасности со стороны персонала должны оперативно рассматриваться руководством для принятия дисциплинарных мер вплоть до увольнения.

Дополнительная информация. Конкретным группам исполнителей могут потребоваться для ознакомления какие-то дополнительные документы, в частности документы специализированных политик и процедур безопасности, а также другие руководящие указания. Необходимость в дополнительных документах политик безопасности в значитель-

ной степени зависит от размеров и сложности организации. Для достаточно большой организации могут потребоваться в дополнение к базовой политике специализированные политики безопасности. Организации меньшего размера нуждаются только в некотором подмножестве специализированных политик. Многие из этих документов поддержки могут быть довольно краткими — объемом в одну-две страницы.

С практической точки зрения политики безопасности можно разделить на три уровня: верхний, средний и нижний [6, 7].

Верхний уровень политики безопасности определяет решения, затрагивающие организацию в целом. Эти решения носят весьма общий характер и исходят, как правило, от руководства организации.

Такие решения могут включать в себя следующие элементы:

- формулировку целей, которые преследует организация в области информационной безопасности, определение общих направлений в достижении этих целей;
- формирование или пересмотр комплексной программы обеспечения информационной безопасности, определение лиц, ответственных за продвижение программы;
- обеспечение материальной базы для соблюдения законов и правил;
- формулировку управленческих решений по вопросам реализации программы безопасности, которые должны рассматриваться на уровне организации в целом.

Политика безопасности верхнего уровня формулирует цели организации в области информационной безопасности в терминах целостности, доступности и конфиденциальности. Если организация отвечает за поддержание критически важных баз данных, на первом плане должна стоять *целостность* данных. Для организации, занимающейся продажами, важна актуальность информации о предоставляемых услугах и ценах, а также ее *доступность* максимальному числу потенциальных покупателей. Режимная организация в первую очередь будет заботиться о *конфиденциальности* информации, т. е. о ее защите от несанкционированного доступа.

На верхний уровень выносится управление ресурсами безопасности и координация использования этих ресурсов, выделение специального персонала для защиты критически важных систем, поддержание контактов с другими организациями, обеспечивающими или контролирующими режим безопасности.

Политика верхнего уровня должна четко определять сферу своего влияния. Это могут быть все компьютерные системы организации или даже больше, если политика регламентирует некоторые аспекты использования сотрудниками своих домашних компьютеров. Возможна и такая ситуация, когда в сферу влияния включаются лишь наиболее важные системы.

В политике должны быть определены обязанности должностных лиц по выработке программы безопасности и по проведению ее в жизнь, т. е. политика может служить основой подотчетности персонала.

Политика верхнего уровня имеет дело с тремя аспектами законопослушности и исполнительской дисциплины. Во-первых, организация должна соблюдать существующие законы. Во-вторых, следует контролировать действия лиц, ответственных за выработку программы безопасности. В-третьих, необходимо обеспечить исполнительскую дисциплину персонала с помощью системы поощрений и наказаний.

Средний уровень политики безопасности определяет решение вопросов, касающихся отдельных аспектов информационной безопасности, но важных для различных систем, эксплуатируемых организацией.

Примеры таких вопросов — отношение к доступу в Интернет (проблема сочетания свободы получения информации с защитой от внешних угроз), использование домашних компьютеров и т. д.

Политика безопасности среднего уровня должна определять для каждого аспекта информационной безопасности следующие моменты:

- *описание аспекта* — позиция организации может быть сформулирована в достаточно общем виде, как набор целей, которые преследует организация в данном аспекте;
- *область применения* — следует специфицировать, где, когда, как, по отношению к кому и чему применяется данная политика безопасности;
- *роли и обязанности* — документ должен содержать информацию о должностных лицах, отвечающих за проведение политики безопасности в жизнь;
- *санкции* — политика должна содержать общее описание запрещенных действий и наказаний за них;
- *точки контакта* — должно быть известно, куда следует обращаться за разъяснениями, помощью и дополнительной информацией. Обычно точкой контакта служит должностное лицо.

Нижний уровень политики безопасности относится к конкретным сервисам. Эта политика включает в себя два аспекта — цели и правила их достижения, поэтому ее порой трудно отделить от вопросов реализации. В отличие от двух верхних уровней, рассматриваемая политика должна быть более детальной.

Приведем несколько примеров вопросов, на которые следует дать ответ при следовании политике безопасности нижнего уровня:

- кто имеет право доступа к объектам, поддерживаемым сервисом;
- при каких условиях можно читать и модифицировать данные;
- как организован удаленный доступ к сервису.

Политика безопасности нижнего уровня может исходить из соображений целостности, доступности и конфиденциальности, но она не должна ими ограничиваться. В общем случае цели должны связывать между собой объекты сервиса и осмысленные действия с ними.

Из целей выводятся правила безопасности, описывающие, кто, что и при каких условиях может делать. Чем детальнее правила, чем более четко и формально они изложены, тем проще поддержать их выполнение программно-техническими мерами. Обычно наиболее формально задаются права доступа к объектам.

Приведем более детальное описание обязанностей каждой категории персонала.

Руководители подразделений отвечают за доведение положений политики безопасности до пользователей. Они обязаны:

- постоянно держать в поле зрения вопросы безопасности. Следить за тем, чтобы то же делали их подчиненные;
- проводить анализ рисков, выявляя активы, требующие защиты, и уязвимые места систем, оценивая размер возможного ущерба от нарушения режима безопасности и выбирая эффективные средства защиты;
- организовать обучение персонала мерам безопасности. Обратить особое внимание на вопросы, связанные с антивирусным контролем;
- информировать администраторов локальной сети и сервисов об изменении статуса каждого из подчиненных (переход на другую работу, увольнение и т. п.);
- обеспечить, чтобы каждый компьютер в их подразделениях имел хозяина или системного администратора, отвечающего за безопасность и обладающего достаточной квалификацией для выполнения этой роли.

Администраторы локальной сети обеспечивают непрерывное функционирование сети и отвечают за реализацию технических мер, необходимых для проведения в жизнь политики безопасности. Они обязаны:

- обеспечить защиту оборудования локальной сети, в том числе интерфейсов с другими сетями;
- оперативно и эффективно реагировать на события, таящие угрозу. Информировать администраторов сервисов о попытках нарушения защиты;
- использовать проверенные средства аудита и обнаружения подозрительных ситуаций. Ежедневно анализировать регистрационную информацию, относящуюся к сети в целом и к файловым серверам в особенности;
- не злоупотреблять своими большими полномочиями. Пользователи имеют право на тайну;
- разработать процедуры и подготовить инструкции для защиты локальной сети от вредоносного программного обеспечения. Оказывать помощь в обнаружении и ликвидации вредоносного кода;
- регулярно выполнять резервное копирование информации, хранящейся на файловых серверах;
- выполнять все изменения сетевой аппаратно-программной конфигурации;
- гарантировать обязательность процедуры идентификации и аутентификации для доступа к сетевым ресурсам. Выделять пользователям входные имена и начальные пароли только после заполнения регистрационных форм;
- периодически производить проверку надежности защиты локальной сети. Не допускать получения привилегий неавторизованными пользователями.

Администраторы сервисов отвечают за конкретные сервисы и, в частности, за то, чтобы защита была построена в соответствии с общей политикой безопасности. Они обязаны:

- управлять правами доступа пользователей к обслуживаемым объектам;
- оперативно и эффективно реагировать на события, таящие угрозу. Оказывать помощь в отражении угрозы, выявлении нарушителей и предоставлении информации для их наказания;
- регулярно выполнять резервное копирование информации, обрабатываемой сервисом;
- выделять пользователям входные имена и начальные пароли только после заполнения регистрационных форм;
- ежедневно анализировать регистрационную информацию, относящуюся к сервису. Регулярно контролировать сервис на предмет вредоносного программного обеспечения;
- периодически производить проверку надежности защиты сервиса. Не допускать получения привилегий неавторизованными пользователями.

Пользователи обязаны работать с локальной сетью в соответствии с политикой безопасности, подчиняться распоряжениям лиц, отвечающих за отдельные аспекты безопасности, ставить в известность руководство обо всех подозрительных ситуациях. Они обязаны:

- знать и соблюдать законы, правила, принятые в данной организации, политику безопасности, процедуры безопасности. Использовать доступные защитные механизмы для обеспечения конфиденциальности и целостности своей информации;
- использовать механизм защиты файлов и должным образом задавать права доступа;
- выбирать качественные пароли, регулярно менять их. Не записывать пароли на бумаге, не сообщать их другим лицам;
- информировать администраторов или руководство о нарушениях безопасности и иных подозрительных ситуациях;
- не использовать слабости в защите сервисов и локальной сети в целом. Не совершать неавторизованной работы с данными, не создавать помех другим пользователям;
- всегда сообщать корректную идентификационную и аутентификационную информацию, не пытаться работать от имени других пользователей;
- обеспечивать резервное копирование информации с жесткого диска своего компьютера;
- знать принципы работы вредоносного программного обеспечения, пути его проникновения и распространения. Знать и соблюдать процедуры для предупреждения проникновения вредоносного кода, его обнаружения и уничтожения;
- знать и соблюдать правила поведения в экстренных ситуациях, последовательность действий при ликвидации последствий аварий.

Управленческие меры обеспечения информационной безопасности. Главной целью мер, предпринимаемых на управленческом уровне, является формирование программы работ в области информационной безопасности и обеспечение ее выполнения путем выделения необходимых ресурсов и осуществления регулярного контроля состояния дел. Основой этой программы является многоуровневая политика безопасности, отражающая комплексный подход организации к защите своих ресурсов и информационных активов.

3.2. Структура политики безопасности организации

Для большинства организаций политика безопасности абсолютно необходима. Политика безопасности определяет отношение организации к обеспечению безопасности и необходимые действия организации по защите своих ресурсов и активов. На основе политики безопасности устанавливаются необходимые средства и процедуры безопасности, а также определяются роли и ответственность сотрудников организации в обеспечении безопасности.

Обычно политика безопасности организации включает следующие компоненты:

- базовая политика безопасности;
- процедуры безопасности;
- специализированные политики безопасности (рис. 3.1).

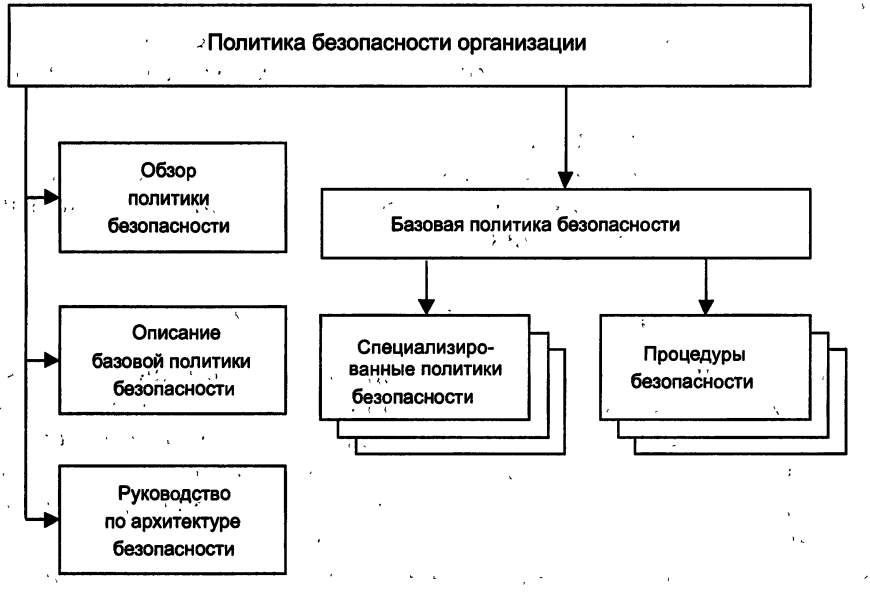


Рис. 3.1. Структура политики безопасности организации

Основные положения политики безопасности организации описываются в следующих документах:

- обзор политики безопасности;
- описание базовой политики безопасности;
- руководство по архитектуре безопасности.

Главным компонентом политики безопасности организации является базовая политика безопасности [7].

3.2.1. Базовая политика безопасности

Базовая политика безопасности устанавливает, как организация обрабатывает информацию, кто может получить к ней доступ и как это можно сделать. В описании базовой политики безопасности определяются разрешенные и запрещенные действия, а также указываются необходимые средства управления в рамках реализуемой архитектуры безопасности. С базовой политикой безопасности согласовываются специализированные политики и процедуры безопасности.

Нисходящий подход, реализуемый базовой политикой безопасности, дает возможность постепенно и последовательно выполнять работу по созданию системы безопасности, не пытаясь сразу выполнить ее целиком. Базовая политика позволяет в любое время ознакомиться с политикой безопасности в полном объеме и выяснить текущее состояние безопасности в организации.

Обзор политики безопасности раскрывает цель политики безопасности, описывает ее структуру, подробно излагает, кто и за что отвечает, устанавливает процедуры и предполагаемые временные рамки для внесения изменений. В зависимости от масштаба организации политика безопасности может содержать больше или меньше разделов.

Руководство по архитектуре безопасности описывает реализацию механизмов безопасности в компонентах архитектуры, используемых в сети организации.

Как отмечалось выше, структура и состав политики безопасности зависят от размера и целей компании. Обычно базовая политика безопасности организации поддерживается набором специализированных политик и процедур безопасности.

3.2.2. Специализированные политики безопасности

Потенциально существуют десятки специализированных политик, которые могут применяться большинством организаций среднего и большого размера. Некоторые политики предназначаются для каждой организации, другие специфичны для определенных компьютерных окружений.

С учетом особенностей применения специализированные политики безопасности можно разделить на две группы:

- политики, затрагивающие значительное число пользователей;
- политики, связанные с конкретными техническими областями.

К специализированным политикам, затрагивающим значительное число пользователей, относятся:

- политика допустимого использования;
- политика удаленного доступа к ресурсам сети;
- политика защиты информации;
- политика защиты паролей и др.

К специализированным политикам, связанным с конкретными техническими областями, относятся:

- политика конфигурации межсетевых экранов;
- политика по шифрованию и управлению криптоключами;
- политика безопасности виртуальных защищенных сетей VPN;
- политика по оборудованию беспроводной сети и др.

Рассмотрим подробнее некоторые из ключевых специализированных политик.

Политика допустимого использования. Базовая политика безопасности обычно связана с рядом политик допустимого использования. Целью политики допустимого использования является установление стандартных норм безопасного использования компьютерного оборудования и сервисов в компании, а также соответствующих мер безопасности сотрудников с целью защиты корпоративных ресурсов и собственной информации. Неправильное использование компьютерного оборудования и сервисов подвергает компанию рискам, включая вирусные атаки, компрометацию сетевых систем и сервисов. Конкретный тип и количество политик допустимого использования зависят от результатов анализа требований бизнеса, оценки рисков и корпоративной культуры в организации.

Политика допустимого использования применяется к сотрудникам, консультантам, временным служащим и другим работникам в компании, включая сотрудников сторонних организаций. Политика допустимого использования предназначается в основном для конечных пользователей. Эта политика указывает пользователям, какие действия разрешаются, а какие запрещены.

Политика допустимого использования должна установить:

- ответственность пользователей за защиту любой информации, используемой и/или хранимой их компьютерами;
- возможность читать и копировать файлы, которые не являются собственными документами пользователей, но доступны им;
- уровень допустимого использования для электронной почты и Web-доступа.

Существует много видов политики допустимого использования. В частности, могут быть политики допустимого использования для компьютеров, передачи данных, коммуникаций электронной почты, портативных персональных компьютеров, веб-доступа и др.

Для образовательных и государственных учреждений политика допустимого использования, по существу, просто обязательна. Без зафиксированной в соответствующем документе политики допустимого использования штатные сотрудники управления и поддержки сети не имеют формальных оснований для применения санкций к своему или

стороннему сотруднику, который допустил грубое нарушение правил безопасной работы на компьютере или в сети.

Для политики допустимого использования не существует специального формата. В этой политике должно быть указано имя сервиса, системы или подсистемы (например, политика использования компьютера, электронной почты, портативных компьютеров и паролей) и описано в самых четких терминах разрешенное и запрещенное поведение. В этой политике должны быть также подробно описаны последствия нарушения ее правил и санкции, налагаемые на нарушителя.

Разработка политики допустимого использования выполняется квалифицированными специалистами по соответствующему сервису, системе или подсистеме под контролем комиссии (команды), которой поручена разработка политики безопасности организации.

Политика удаленного доступа. Целью политики удаленного доступа является установление стандартных норм безопасного удаленного соединения любого хоста с сетью компании. Эти стандартные нормы призваны минимизировать ущерб компании из-за возможного неавторизованного использования ресурсов компании. К такому ущербу относятся утрата интеллектуальной собственности компании, потеря конфиденциальных данных, искажение имиджа компании, повреждения критических внутренних систем компании и т. д.

Эта политика касается всех сотрудников, поставщиков и агентов компании при использовании ими для удаленного соединения с сетью компании компьютеров или рабочих станций, являющихся собственностью компании либо находящихся в личной собственности.

Политика удаленного доступа:

- намечает и определяет допустимые методы удаленного соединения с внутренней сетью;
- существенна в большой организации, где сети территориально распределены и простираются до домов;
- должна охватывать по возможности все распространенные методы удаленного доступа к внутренним ресурсам.

Политика удаленного доступа должна определить:

- какие методы разрешаются для удаленного доступа;
- каковы ограничения на данные, к которым можно получить удаленный доступ;
- кто может иметь удаленный доступ.

Защищенный удаленный доступ должен быть строго контролируемым. Применяемая процедура контроля должна гарантировать, что доступ к надлежащей информации или сервисам получат только прошедшие проверку люди. Сотрудник компании не должен передавать свои логин и пароль никогда и никому, включая членов своей семьи. Управление удаленным доступом не должно быть настолько сложным, чтобы это приводило к возникновению ошибок.

Контроль доступа целесообразно выполнять с помощью одноразовой парольной аутентификации или с помощью открытых/секретных ключей (см. главы 4 и 5).

Сотрудники компании с правами удаленного доступа должны обеспечить, чтобы принадлежащие им или компании персональный компьютер либо рабочая станция, которые удаленно подсоединены к корпоративной сети компании, не были связаны в это же время с какой-либо другой сетью, за исключением персональных сетей, находящихся под полным контролем пользователя.

Сотрудники компании с правами удаленного доступа к корпоративной сети компании должны обеспечить, чтобы их соединение удаленного доступа имело такие же характеристики безопасности, как обычное локальное соединение с компанией.

Все хосты, которые подключены к внутренним сетям компании с помощью технологий удаленного доступа, должны использовать самое современное антивирусное обеспечение, это требование относится и к персональным компьютерам компании.

Любой сотрудник компании, уличенный в нарушении данной политики, может быть подвергнут дисциплинарному взысканию вплоть до увольнения с работы.

3.2.3. Процедуры безопасности

Процедуры безопасности важны не менее, чем политики. Процедуры безопасности являются необходимым и важным дополнением к политикам безопасности. Политики безопасности только описывают, что должно быть защищено и каковы основные правила защиты. Процедуры безопасности определяют, как защитить ресурсы и каковы механизмы исполнения политики, т. е. как реализовывать политики безопасности.

По существу, процедуры безопасности представляют собой пошаговые инструкции для выполнения оперативных задач. Часто процедура является тем инструментом, с помощью которого политика преобразуется в реальное действие. Например, политика паролей формулирует правила конструирования паролей, правила о том, как защитить ваш пароль и как часто заменять пароли. Процедура управления паролями описывает процессы создания новых паролей, распределения их, а также гарантированной смены паролей на критичных устройствах.

Процедуры безопасности детально определяют действия, которые нужно предпринять при реагировании на конкретные события. Процедуры безопасности обеспечивают быстрое реагирование в критической ситуации. Процедуры помогают устранить проблему единой точки отказа в работе, если, например, во время кризиса работник неожиданно покидает рабочее место или оказывается недоступен.

Многие процедуры, связанные с безопасностью, должны быть стандартными средствами в любом подразделении. В качестве примеров можно указать процедуры для резервного копирования и внесистемного хранения защищенных копий, а также процедуры для вывода поль-

зователя из активного состояния и/или архивирования его логина и пароля, применяемые сразу, как только данный пользователь увольняется из организации.

Рассмотрим несколько важных процедур безопасности, которые необходимы почти каждой организации.

Процедура реагирования на события. Данная процедура является необходимым средством безопасности для большинства организаций. Организация особенно уязвима, когда обнаруживается вторжение в ее сеть или когда она сталкивается со стихийным бедствием. Нетрудно представить, что произойдет в последующие минуты и часы, если интеллектуальная собственность компании составляет миллионы или миллиарды долларов.

Процедуру реагирования на события иногда называют *процедурой обработки событий* или *процедурой реагирования на инциденты*. Практически невозможно указать отклики на все события нарушений безопасности, но нужно стремиться охватить основные типы нарушений, которые могут произойти.

Вот некоторые примеры нарушений безопасности: сканирование портов сети, атака типа «отказ в обслуживании», компрометация хоста, несанкционированный доступ и др.

Данная процедура определяет:

- каковы обязанности членов команды реагирования;
- какую информацию следует регистрировать и прослеживать;
- как обрабатывать исследование отклонений от нормы и атаки вторжения;
- кого уведомлять и когда;
- кто может выпускать в свет информацию и какова процедура ее выпуска;
- как должен выполняться последующий анализ и кто будет в этом участвовать.

В команду реагирования могут быть включены должностные лица компании, менеджер отдела маркетинга (для связи с прессой), системный и сетевой администраторы и представитель соответствующих правоохранительных органов. Процедура должна указать, когда и в каком порядке они вызываются.

Процедура управления конфигурацией. Процедура управления конфигурацией обычно определяется на корпоративном уровне или уровне подразделения. Эта процедура должна определить процесс документирования и запроса изменений конфигурации на всех уровнях принятия решений. В принципе, должна существовать центральная группа, которая рассматривает все запросы на изменения конфигурации и принимает необходимые решения.

Процедура управления конфигурацией определяет:

- кто имеет полномочия выполнять изменения конфигурации аппаратного и программного обеспечения;
- как тестируется и инсталлируется новое аппаратное и программное обеспечение;

- как документируются изменения в аппаратном и программном обеспечении;
- кто должен быть проинформирован, когда вносятся изменения в аппаратном и программном обеспечении.

Процесс управления конфигурацией важен по нескольким причинам:

- он документирует внесенные изменения и обеспечивает возможность аудита;
- он документирует возможный простой системы;
- он дает способ координировать изменения так, чтобы одно изменение не помешало другому.

3.3. Разработка политики безопасности организации

Разработка политики безопасности является ключевым этапом построения защищенной информационной системы или сети. Следует отметить, что составление политики безопасности или политик является только началом осуществления общей программы обеспечения безопасности организации. Детальная программа обеспечения безопасности необходима для создания эффективной системы безопасности организации на основе разработанной политики безопасности.

Ниже перечислены основные этапы программы обеспечения безопасности:

- определение ценности технологических и информационных активов организации;
- оценка рисков этих активов (сначала путем идентификации тех угроз, для которых каждый актив является целевым объектом, а затем оценкой вероятности того, что эти угрозы будут реализованы на практике);
- установление уровня безопасности, определяющего защиту каждого актива, т. е. мер безопасности, которые можно считать рентабельными для применения;
- формирование на базе предыдущих этапов политики безопасности организации;
- привлечение необходимых финансовых ресурсов для реализации политики безопасности, приобретение и установка требуемых средств безопасности;
- проведение разъяснительных мероприятий и обучения персонала для поддержки сотрудниками и руководством требуемых мер безопасности;
- регулярный контроль пошаговой реализации плана безопасности с целью выявления текущих проблем, учета изменения внешнего окружения и внесение необходимых изменений в состав персонала.

Опыт показал, что в целом организации получают существенную выгоду от реализации хорошо разработанной методологии решения указанных выше задач.

К политикам безопасности предъявляются следующие основные требования:

- политики безопасности должны:
  - указывать цели и причины, по которым нужна политика;
  - описывать, что именно охватывается этими политиками;
  - определить роли, обязанности и контакты;
  - определить, как будут обрабатываться нарушения безопасности;
- политики безопасности должны быть:
  - реальными и осуществимыми;
  - краткими и доступными для понимания;
  - сбалансированными по защите и производительности [11].

Первыми шагами по разработке политики безопасности являются следующие:

- создание команды по разработке политики;
- принятие решения об области действия и целях политики;
- принятие решения об особенностях разрабатываемой политики;
- определение лица или органа для работы в качестве официального интерпретатора политики.

Ко всем разрабатываемым политикам безопасности целесообразно применять унифицированный процесс проектирования с единообразными требованиями к политикам.

Одним из первых шагов является *создание команды по разработке политики безопасности организации.* Иногда эту команду называют группой, комиссией или комитетом. Команда создается руководством организации, которое должно осознавать важность информационной безопасности и полностью реализовать свою позитивную роль в успешной разработке, принятии и внедрении этой политики.

В состав команды следует включать квалифицированных специалистов, хорошо разбирающихся в требованиях бизнеса, информационных технологиях и безопасности, юриста и члена руководства, который сможет проводить в жизнь эту политику безопасности. К работе этой команды должны быть также привлечены администраторы безопасности и системные администраторы, представитель от сообщества пользователей.

Размер команды по разработке политики зависит от масштаба и области действия политики. Крупномасштабные политики могут потребовать команды из 5—10 человек, в то время как политики небольшого масштаба могут потребовать только одного или двух человек.

Как только создана такая команда, ее первым шагом является *анализ требований бизнеса.* Члены команды с различными позициями и точками зрения должны проанализировать требования бизнеса к использованию компьютерных и сетевых сервисов. Когда мнения некоторых членов этой команды не совпадают, столкновения их интересов и

пересечения разных отраслей знания при обсуждении требований бизнеса позволяют получить более полную и объективную картину, чем при обычном опросе людей, работающих в области маркетинга, продаж или разработки [7].

На этом этапе анализируются и решаются следующие вопросы. Какие компьютерные и сетевые сервисы требуются для бизнеса и как эти требования могут быть удовлетворены при условии обеспечения безопасности? Сколько сотрудников зависят от доступа в Интернет, использования электронной почты и доступности интранет-сервисов? Зависят ли компьютерные и сетевые сервисы от удаленного доступа к внутренней сети? Имеются ли требования по доступу к Веб? Требуются ли клиентам данные технической поддержки через Интернет? При анализе каждого сервиса следует обязательно спрашивать: «Имеется ли требование бизнеса на этот сервис?» Это самый важный вопрос.

После анализа и систематизации требований бизнеса команда по разработке политики безопасности переходит к анализу и оценке рисков. Использование информационных систем и сетей связано с определенной совокупностью рисков. *Анализ рисков* является важнейшим этапом формирования политики безопасности (рис. 3.2). Иногда этот этап называют также *анализом уязвимостей* или *оценкой угроз*. Хотя эти термины имеют несколько различающиеся толкования, конечные результаты сходны.

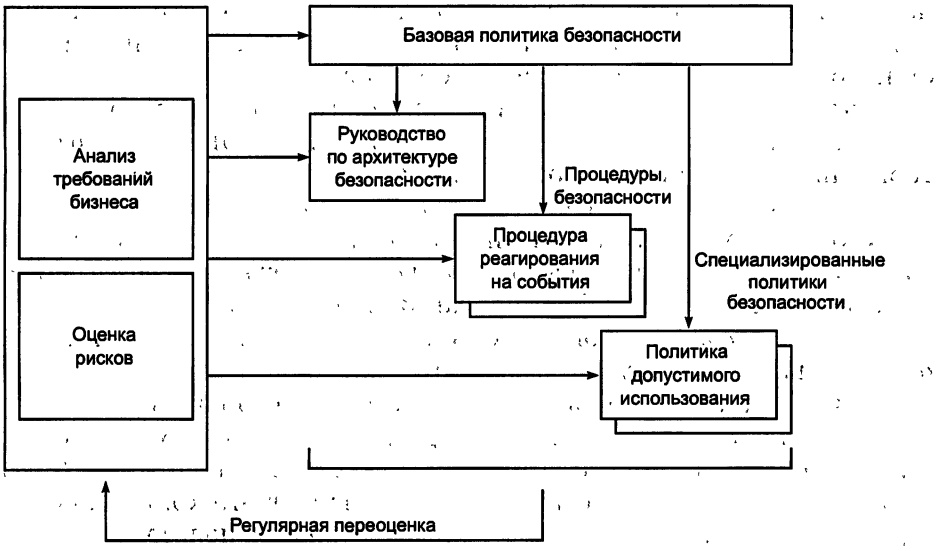


Рис. 3.2. Схема разработки политики безопасности

На этапе анализа рисков осуществляются следующие действия:

- идентификация и оценка стоимости технологических и информационных активов;
- анализ тех угроз, для которых данный актив является целевым объектом;

- оценка вероятности того, что угроза будет реализована на практике;
- оценка рисков этих активов [4].

Оценка риска выявляет как наиболее ценные, так и наиболее уязвимые активы, она позволяет точно установить, на какие проблемы нужно обратить особое внимание. Отчет об оценке рисков является ценным инструментом при формировании политики сетевой безопасности.

После оценки рисков активов можно переходить к *установлению уровня безопасности*, определяющего защиту каждого актива, т. е. *мер безопасности*, которые можно считать рентабельными для применения.

В принципе, *стоимость защиты конкретного актива не должна превышать стоимости самого актива.* Необходимо составить подробный перечень всех активов, который включает такие материальные объекты, как серверы и рабочие станции, и такие нематериальные объекты, как данные и программное обеспечение. Должны быть идентифицированы директории, которые содержат конфиденциальные файлы или файлы целевого назначения. После идентификации этих активов должно быть проведено определение стоимости замены каждого актива с целью назначения приоритетов в перечне активов.

Для контроля эффективности деятельности в области безопасности и для учета изменений обстановки необходима *регулярная переоценка рисков.*

После проведения описанной выше работы можно переходить к непосредственному составлению политики безопасности. В политике безопасности организации должны быть определены используемые стандарты, правила и процессы безопасности.

Стандарты указывают, каким критериям должно следовать управление безопасностью. *Правила* подробно описывают принципы и способы управления безопасностью. *Процессы* должны осуществлять точную реализацию правил в соответствии с принятыми стандартами.

Кроме того, политика безопасности должна определить значимые для безопасности *роли* и указать *ответственности этих ролей.* Роли устанавливаются во время формирования процессов [7].

Обычно *процесс* состоит из одного или более действий, где каждое *действие* включает четыре компонента (рис. 3.3):

1. *Вход*, например запрос пользователем нового пароля.

2. *Механизм*, который реализует данное действие и указывает средства или роли, с помощью которых это действие выполняется. Другими словами, он определяет, какие роли вовлечены в это конкретное действие. В нашем примере такими ролями являются пользователь, запрашивающий новый пароль, и администратор безопасности.

3. *Управление* — описывает алгоритм или условия, которые управляют этим действием. Например, стандарт может задать следующее условие: при запросе нового пароля инициатор запроса должен успешно пройти аутентификацию.

4. *Выход* — является результатом этого действия. В нашем примере таким выходом является сообщение пользователю нового пароля.

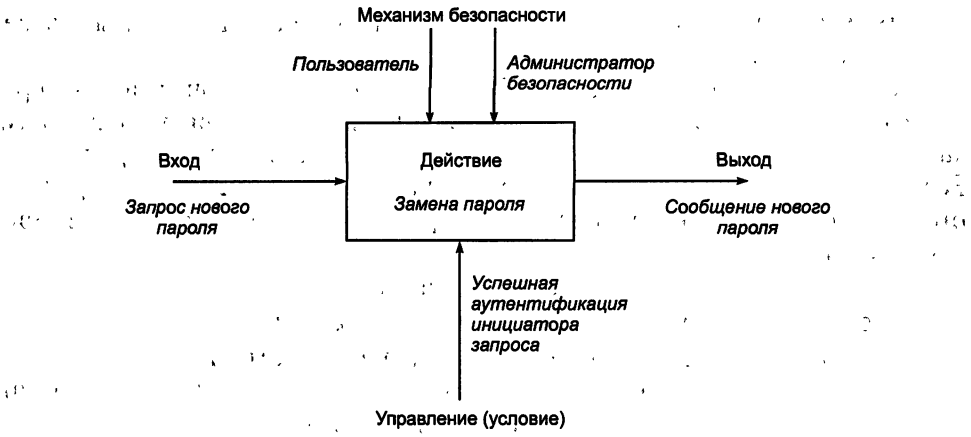


Рис. 3.3. Графическое представление действия в рамках процесса

Связывая вместе все действия, входящие в процесс, мы получаем точное представление результирующего процесса и ролей, необходимых для его исполнения. В данном примере процесс состоит из одного действия — обновления пароля пользователя; роли идентифицируются как Пользователь и Администратор безопасности. Стандарты, правила и процессы должны быть документированы в рамках политики для целей аудита.

Компоненты архитектуры безопасности

Руководство по архитектуре безопасности детально определяет контрмеры против угроз, раскрытых при оценке рисков. Это руководство описывает компоненты архитектуры безопасности сети, рекомендует конкретные продукты безопасности и дает инструкции, как их развернуть и управлять ими. В частности, это руководство может содержать рекомендации, где следует поставить межсетевые экраны, когда использовать шифрование, где разместить веб-серверы и как организовать управление коммуникациями с бизнес-партнерами и заказчиками. Руководство по архитектуре безопасности определяет также гарантии безопасности, аудит и средства контроля.

Рассмотрим для примера некоторые компоненты архитектуры безопасности сети.

Физическая безопасность. Обеспечение физической безопасности особенно важно, когда заполнение физической области, где находятся системные компоненты, очень неоднородно. Наличие в здании компании не только своих сотрудников, но и людей из других компаний, таких как заказчики, партнеры или клиенты, является наиболее распространенной ситуацией, которая требует физической защиты компьютерной среды.

Физическая защита ресурсов и активов организации достигается с помощью аппаратных средств и размещения соответствующих компью-

терных и коммуникационных средств в физически защищенных помещениях или зонах.

Без обеспечения физической безопасности будут подвергаться серьезным угрозам такие важные аспекты информационной безопасности, как конфиденциальность, доступность и целостность информации. Реализация физической защиты заключается прежде всего в определении тех компонентов компьютерной среды, которые должны быть физически защищены.

Перечень таких компонентов должен включать:

- центральные процессоры и системные блоки;
- компоненты инфраструктуры локальной сети LAN, такие как системы управления LAN, мосты, маршрутизаторы, коммутационные коммутаторы, активные порты и др.;
- системы, связанные с LAN;
- медиапамять.

Затем необходимо установить два или три типа областей с различными уровнями безопасности, такими как:

- *открытые области*, в которые могут допускаться все сотрудники компьютерной среды;
- *контролируемые области*, которые могут и должны быть закрыты, когда находятся без присмотра;
- *особо контролируемые области*, куда ограничен доступ даже зарегистрированным авторизованным пользователям.

Далее каждая такая область назначается одному компоненту системы или топологии системных компонентов в зависимости от степени их конфиденциальности.

Логическая безопасность характеризует уровень защиты ресурсов и активов в сети. Логическая безопасность включает средства безопасности, осуществляющие идентификацию и аутентификацию пользователей, управление доступом, межсетевое экранирование, аудит и мониторинг сети, управление удаленным доступом и т. д.

Защита ресурсов. Ресурсы (файлы, базы данных, программы, данные) могут быть разделены на две группы:

1. *Ресурсы операционной системы* представляют собой те объекты данных, которые связаны с системными сервисами или функциями; они включают системные программы и файлы, подсистемы и программные продукты.

Ресурсы операционной системы обычно находятся под управлением и ответственностью провайдера сервиса. Их целостность должна гарантироваться, поскольку эти данные критичны для того сервиса, который организация хочет поставлять.

Ресурсы операционной системы не всегда являются ограниченными для чтения, хотя список исключений должен быть установлен и соответственно защищен. Типичным примером такого исключения является база данных, в которой хранятся пароли и идентификаторы пользователя.

2. *Ресурсы пользователей* представляют собой те объекты данных, которые связаны с отдельными пользователями или группами пользователей. Ресурсы пользователей должны быть защищены в соответствии с требованиями собственника данных. Для гарантии хотя бы минимального уровня безопасности рекомендуется установить по умолчанию некоторую начальную защиту этих ресурсов.

Определение административных полномочий. Некоторые из пользователей, находящихся в сети, имеют особые полномочия. Такие полномочия нужны для управления компьютерными системами и безопасностью. Эти административные полномочия можно разделить на две категории:

- полномочия системного администратора;
- полномочия администратора безопасности.

Полномочия системного администратора позволяют администратору выполнить все действия, необходимые для управления компьютерными системами. Эти полномочия могут дать возможность администратору обойти контроль безопасности, но это должно рассматриваться как злоупотребление полномочиями.

Полномочия администратора безопасности дают возможность администратору выполнять действия, необходимые для управления безопасностью. Эти полномочия позволяют администратору осуществлять изменение системных компонентов или считывать конфиденциальные данные. Однако, если считывание конфиденциальных данных выполнено администратором без соответствующей потребности бизнеса, это должно рассматриваться как злоупотребление своими полномочиями.

Полномочия системного администратора и администратора безопасности являются одинаково важными для безопасности. С учетом этого необходимо выполнить следующее:

- определить для каждой системной платформы или системы управления доступом те полномочия, которые могут быть признаны в указанных категориях;
- назначить полномочия администраторам в соответствии с индивидуальной ответственностью;
- периодически проверять назначение идентификаторов авторизованным пользователям.

Роли и ответственности в безопасности сети

Число устанавливаемых ролей зависит от количества реализуемых процессов безопасности в организации. Во многих организациях можно найти одни и те же типы ролей. Рассмотрим перечень обычно устанавливаемых ролей:

- *провайдер сервисов* — менеджер группы и/или организации, который предоставляет сервисы обработки информации. Обычно эта организация отвечает за обеспечение безопасности компьютерной среды;

- *менеджер данных* — менеджер, отвечающий за управление безопасностью распределяемых данных. В круг ответственности менеджера данных входят:
  - оценка уровня конфиденциальности данных с целью их классификации;
  - установление определенного уровня защиты (в соответствии с этой классификацией);
  - разрешение или запрет на доступ к данным под его личную ответственность;
- *аудитор* — это лицо, ответственное за:
  - исполнение политик безопасности;
  - исполнение процессов безопасности;
  - периодическое выполнение контрольной оценки безопасности;
  - задание требований для приложений/инструментов/решений в целях обеспечения требуемой безопасности;
- *администратор безопасности* — это лицо, ответственное за настройку и управление системных средств управления безопасностью. В круг ответственности администратора безопасности входят следующие обязанности:
  - обеспечение настройки безопасности системы в соответствии со стандартами и правилами, т. е. администратор безопасности отвечает за установку системных политик, включая парольную политику, политику аудита, политику входа в систему и стандартный доступ к типам ресурсов;
  - управление атрибутами доступа пользователей путем замены паролей, определения новых и удаления старых идентификаторов пользователей;
  - выполнение периодических проверок с целью контроля состояния безопасности компьютерной среды;
- *пользователь данными* — в обязанности пользователя данными входят:
  - исполнение инструкций безопасности. Например, пароль должен быть нетривиальным и удовлетворять утвержденным синтаксическим правилам. Это нужно применять в любой системе, независимо от существующего управления безопасностью;
  - использование своих полномочий доступа и системных полномочий только для разрешенного администрацией применения.

Каждый пользователь компьютерной среды является пользователем данными.

Аудит и оповещение. Под термином *«аудит»* подразумевается способность регистрировать все важные с точки зрения безопасности действия, выполненные в компьютерной среде. Под термином *«оповещение»* понимают способность оповещать об этих действиях в читабельной форме.

Для безопасности очень важна хорошая схема аудита; она должна всегда давать ясную картину состояния безопасности. Более того, схема аудита является мощным пассивным агентом безопасности. В разде-

ле 2.2 отмечалось, что солидная доля угроз безопасности обусловлена обиженными или нечестными сотрудниками. Эффективное отслеживание активности угроз этого типа с помощью аудита является сильным сдерживающим средством.

При формировании политики аудита нужно учитывать два аспекта:

1. Необходимо решить, какие события особенно важны для безопасности. Регистрация всех событий подряд — не лучший выбор, а просто бесполезное расходование дискового пространства, такая регистрация может вызвать много проблем при генерации отчета.

Вот рекомендация минимального перечня событий для регистрации:

- все нарушения безопасности, такие как:
  - — неавторизованный доступ к системе;
  - — неправильный пароль;
  - — аннулированный пароль;
  - — неавторизованный доступ к ресурсу;
- все попытки доступа к чувствительным/важным областям систем;
- все выдаваемые команды безопасности, использующие административные полномочия;
- все попытки доступа к ресурсам операционных систем, за исключением доступа по умолчанию.

2. Необходимо решить, как долго должны храниться записи регистрации, и составить соответствующий план хранения.

Управление тревожной сигнализацией. Для обеспечения безопасности важно иметь возможность немедленного реагирования, когда предполагается, что компьютерная среда подвергается опасности атаки на систему в попытке получить неавторизованный доступ. Цель состоит в том, чтобы определить в реальном времени, когда возникнет опасность, и выдать сигнал тревоги.

Приведем пример последовательности процессов для обнаружения проблемы и выдачи сигнала тревоги:

- каждое нарушение безопасности должно генерировать системное событие;
- одно системное событие не является неизбежно достаточным, чтобы утверждать, что это опасность; в таком случае подобные события должны накапливаться;
- совокупность таких событий должна затем сравниваться с заранее установленной пороговой величиной;
- если результат этой совокупности превышает пороговую величину, выдается сигнал тревоги.

В результате выполнения этих процессов можно игнорировать неправильный ввод кем-то пароля утром во вторник, но следует обратить внимание, когда кто-то вводит много неправильных паролей, связанных со многими пользовательскими идентификаторами в воскресенье вечером.

Для управления тревожной сигнализацией важно правильное определение ролей и ответственностей и назначение этих ролей и ответственностей соответствующим менеджерам. Система тревожной сигнали-

зации должна не только анализировать тревожную ситуацию и своевременно выдать тревожной сигнал либо инициировать некоторый автоматический процесс, но и оповестить ответственных должностных лиц, способных оперативно принять необходимые меры.

Вопросы для самоконтроля

1. Объясните понятие «политика безопасности организации».
2. Какие разделы должна содержать документально оформленная политика безопасности?
3. Какие проблемы решает верхний уровень политики безопасности?
4. Какие задачи решает средний уровень политики безопасности?
5. Каковы особенности нижнего уровня политики безопасности?
6. Сформулируйте обязанности руководителей подразделений, администраторов и пользователей при реализации политики безопасности.
7. Опишите структуру политики безопасности организации.
8. Что представляют собой специализированные политики безопасности?
9. Приведите несколько примеров специализированных политик безопасности с описанием их особенностей.
10. Что представляют собой процедуры безопасности?
11. Приведите несколько примеров процедур безопасности с описанием их особенностей.
12. Сформулируйте основные этапы разработки политики безопасности организации.

ЧАСТЬ II

ТЕХНОЛОГИИ ЗАЩИТЫ КОРПОРАТИВНЫХ ДАННЫХ

Безопасность корпоративных данных означает их конфиденциальность, целостность и подлинность. Критерии безопасности корпоративных данных могут быть определены следующим образом.

Конфиденциальность данных предполагает их доступность только для тех лиц, которые имеют на это соответствующие полномочия. Под *обеспечением конфиденциальности* информации понимается создание таких условий, при которых понять содержание передаваемых данных может только законный получатель, кому и предназначена данная информация.

Целостность информации предполагает ее неизменность в процессе передачи от отправителя к получателю. Под *обеспечением целостности* информации понимается достижение идентичности отправляемых и принимаемых данных.

Подлинность информации предполагает соответствие этой информации ее явному описанию и содержанию, в частности соответствие действительным характеристикам указанных отправителя, времени отправления и содержания. *Обеспечение подлинности* информации, реализуемое на основе аутентификации, состоит в достоверном установлении отправителя, а также защите информации от изменения при ее передаче от отправителя к получателю. Своевременно обнаруженное нарушение подлинности и целостности полученного сообщения позволяет предотвратить отрицательные последствия, связанные с дальнейшим использованием такого искаженного сообщения.

Большинство средств защиты информации базируется на использовании криптографических шифров и процедур шифрования/расшифрования.

Глава 4
КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Криптография является методологической основой современных систем обеспечения безопасности информации в компьютерных системах и сетях. Исторически криптография (в переводе с греческого этот термин означает «тайнопись») зародилась как способ скрытой передачи сообщений. Криптография представляет собой совокупность методов преобразования данных, направленных на то, чтобы защитить эти данные, сделав их бесполезными для незаконных пользователей. Такие преобразования обеспечивают решение трех главных проблем защиты данных: обеспечение конфиденциальности, целостности и подлинности передаваемых или сохраняемых данных.

4.1. Основные понятия криптографической защиты информации

Для обеспечения безопасности данных необходимо поддерживать три основные функции:

- защиту конфиденциальности передаваемых или хранимых в памяти данных;
- подтверждение целостности и подлинности данных;
- аутентификацию абонентов при входе в систему и при установлении соединения.

Для реализации указанных функций используются криптографические технологии шифрования, цифровой подписи и аутентификации.

Конфиденциальность обеспечивается с помощью алгоритмов и методов симметричного и асимметричного шифрования, а также путем взаимной аутентификации абонентов на основе многоразовых и одноразовых паролей, цифровых сертификатов, смарт-карт и т. п.

Целостность и подлинность передаваемых данных обычно достигается с помощью различных вариантов технологии электронной подписи, основанных на односторонних функциях и асимметричных методах шифрования.

Аутентификация разрешает устанавливать соединения только между легальными пользователями и предотвращает доступ к средствам

сети нежелательных лиц. Абонентам, доказавшим свою легитимность (аутентичность), предоставляются разрешенные виды сетевого обслуживания.

Основой большинства криптографических средств защиты информации является *шифрование данных.*

Под *шифром* понимают совокупность процедур и правил криптографических преобразований, используемых для зашифровывания и расшифровывания информации по ключу шифрования. Под *зашифрованием информации* понимается процесс преобразования открытой информации (исходного текста) в зашифрованный текст (шифртекст). Процесс восстановления исходного текста по криптограмме с использованием ключа шифрования называют *расшифровыванием* (дешифрованием).

Обобщенная схема криптосистемы шифрования показана на рис. 4.1. Исходный текст передаваемого сообщения (или хранимой информации) M зашифровывается с помощью криптографического преобразования E_{k_1} с получением в результате *шифртекста* C:

$$C = E_{k_1}(M),$$

где k_1 — параметр функции E, называемый ключом шифрования.

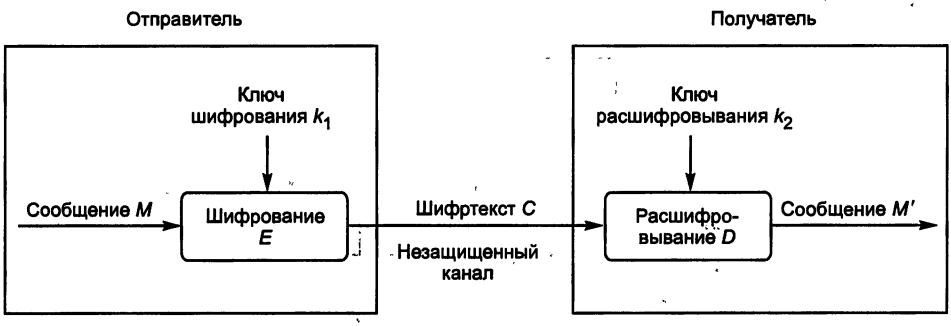


Рис. 4.1. Обобщенная схема криптосистемы шифрования

Шифртекст C, называемый еще *криптограммой*, содержит исходную информацию M в полном объеме, однако последовательность знаков в нем внешне представляется случайной и не позволяет восстановить исходную информацию без знания ключа шифрования k_1.

Ключ шифрования является тем элементом, с помощью которого можно варьировать результат криптографического преобразования. Данный элемент может принадлежать конкретному пользователю или группе пользователей и являться для них уникальным. Зашифрованная с использованием конкретного ключа информация может быть расшифрована только его владельцем (или владельцами).

Обратное преобразование информации выглядит следующим образом:

$$M' = D_{k_2}(C).$$

Функция D является обратной к функции E и производит расшифрование шифртекста. Она также имеет дополнительный параметр в виде ключа k_2. Ключ расшифрования k_2 должен однозначно соответствовать ключу k_1, в этом случае полученное в результате расшифрования сообщение M' будет эквивалентно M. При отсутствии верного ключа k_2 получить исходное сообщение $M' = M$ с помощью функции D невозможно.

Преобразование шифрования может быть симметричным или асимметричным относительно преобразования расшифрования. Соответственно различают два основных класса криптосистем:

- симметричные криптосистемы;
- асимметричные криптосистемы.

Известно несколько классификаций криптографических алгоритмов [45]. Одна из них подразделяет КА в зависимости от числа ключей, применяемых в конкретном алгоритме:

- бесключевые КА — не используют в вычислениях никаких ключей;
- одноключевые КА — работают с одним ключевым параметром (секретным ключом);
- двухключевые КА — на различных стадиях работы в них применяются два ключевых параметра: секретный и открытый ключи.

Существуют более детальные классификации, например показанная на рис. 4.2.

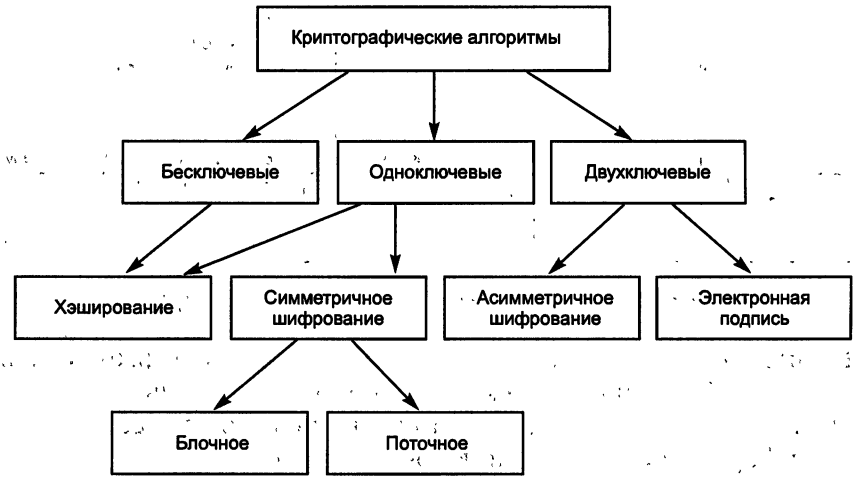


Рис. 4.2. Классификация криптоалгоритмов защиты информации

Охарактеризуем кратко основные типы КА.

Хэширование — это метод криптозащиты, представляющий собой контрольное преобразование информации: из данных неограниченного размера путем выполнения криптографических преобразований вычисляется хэш-значение фиксированной длины, однозначно соответствующее исходным данным. Хэширование может выполняться как с использованием некоторого секретного ключа, так и без него. Такое криптографическое контрольное суммирование широко используется в

различных методах защиты информации, в частности для подтверждения целостности данных, если использование электронной подписи невозможно (например, из-за большой ресурсоемкости) или избыточно. Кроме того, данный метод применяется в схемах электронной подписи («подписывается» обычно хэш-значение данных, а не все данные целиком), а также в схемах аутентификации пользователей (при проверке, действительно ли пользователь является тем, за кого себя выдает).

Симметричное шифрование использует один и тот же ключ как для зашифрования, так и для расшифрования информации. Фактически оба ключа (зашифрования и расшифрования) могут и различаться, но если в каком-либо КА их легко вычислить один из другого в обе стороны, такой алгоритм однозначно относится к симметричному шифрованию.

Симметричное шифрование подразделяется на два вида: блочное и поточное, хотя стоит сразу отметить, что в некоторых классификациях они не разделяются и считается, что поточное шифрование — это шифрование блоков единичной длины.

Блочное шифрование характеризуется тем, что информация предварительно разбивается на блоки фиксированной длины (например, 64 или 128 бит). При этом в различных КА или даже в разных режимах работы одного и того же алгоритма блоки могут шифроваться как независимо друг от друга, так и «со сцеплением» — когда результат шифрования текущего блока данных зависит от значения предыдущего блока или от результата шифрования предыдущего блока.

Поточное шифрование применяется прежде всего тогда, когда информацию невозможно разбить на блоки, — скажем, есть некий поток данных, каждый символ которых требуется зашифровать и отправить, не дожидаясь остальных данных, достаточных для формирования блока. Алгоритмы поточного шифрования шифруют данные побитно или посимвольно.

Асимметричное шифрование характеризуется применением двух типов ключей: открытого — для зашифрования информации — и секретного — для ее расшифрования. Секретный и открытый ключи связаны между собой достаточно сложным соотношением. Главное в этом соотношении — легкость вычисления открытого ключа из секретного и невозможность (за ограниченное время при реальных ресурсах) вычисления секретного ключа из открытого при достаточно большой размерности операндов.

Электронная цифровая подпись (ЭЦП) используется для подтверждения целостности и авторства данных. Как и в случае асимметричного шифрования, в данном методе применяются двухключевые алгоритмы с таким же простым вычислением открытого ключа из секретного и практической невозможностью обратного вычисления. Однако назначение ключей ЭЦП совершенно иное. Секретный ключ применяется для вычисления ЭЦП, открытый ключ необходим для ее проверки. При соблюдении правил безопасного хранения секретного ключа никто, кроме его владельца, не в состоянии вычислить верную ЭЦП какого-либо электронного документа.

4.2. Симметричные криптосистемы шифрования

Исторически первыми появились симметричные криптографические системы. В симметричной криптосистеме шифрования используется один и тот же ключ для зашифрования и расшифрования информации. Это означает, что любой, кто имеет доступ к ключу шифрования, может расшифровать сообщение. Соответственно, с целью предотвращения несанкционированного раскрытия зашифрованной информации все ключи шифрования в симметричных криптосистемах должны держаться в секрете. Именно поэтому симметричные криптосистемы называют криптосистемами с секретным ключом — ключ шифрования должен быть доступен только тем, кому предназначено сообщение. Симметричные криптосистемы называют еще одноключевыми криптографическими системами или криптосистемами с закрытым ключом. Схема симметричной криптосистемы шифрования показана на рис. 4.3.

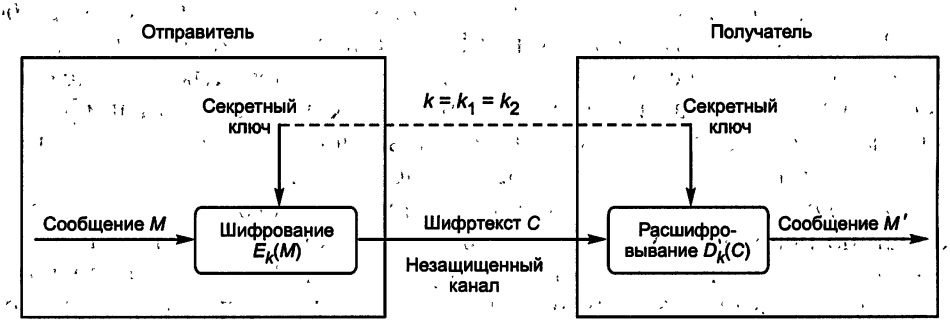


Рис. 4.3. Схема симметричной криптосистемы шифрования

Данные криптосистемы характеризуются наиболее высокой скоростью шифрования, и с их помощью обеспечивается как конфиденциальность и подлинность, так и целостность передаваемой информации.

Конфиденциальность передачи информации с помощью симметричной криптосистемы зависит от надежности шифра и обеспечения конфиденциальности ключа шифрования. Обычно ключ шифрования представляет собой файл или массив данных и хранится на персональном ключевом носителе, например дискете или смарт-карте; обязательно принятие мер, обеспечивающих недоступность персонального ключевого носителя кому-либо, кроме его владельца.

Подлинность обеспечивается за счет того, что без предварительного расшифровывания практически невозможно осуществить смысловую модификацию и подлог криптографически закрытого сообщения. Фальшивое сообщение не может быть правильно зашифровано без знания секретного ключа.

Целостность данных обеспечивается присоединением к передаваемым данным специального кода (имитоприставки), вырабатываемого по секретному ключу. Имитоприставка является разновидностью кон-

трольной суммы, т. е. некоторой эталонной характеристикой сообщения, по которой осуществляется проверка целостности последнего. Алгоритм формирования имитоприставки должен обеспечивать ее зависимость по некоторому сложному криптографическому закону от каждого бита сообщения. Проверка целостности сообщения выполняется получателем сообщения путем выработки по секретному ключу имитоприставки, соответствующей полученному сообщению, и ее сравнения с полученным значением имитоприставки. При совпадении делается вывод о том, что информация не была модифицирована на пути от отправителя к получателю.

Симметричное шифрование идеально подходит для шифрования информации «для себя», например, с целью предотвратить несанкционированный доступ к ней в отсутствие владельца. Это может быть как архивное шифрование выбранных файлов, так и прозрачное (автоматическое) шифрование целых логических или физических дисков.

Обладая высокой скоростью шифрования, одноключевые криптосистемы позволяют решать многие важные задачи защиты информации. Однако автономное использование симметричных криптосистем в компьютерных сетях порождает проблему распределения ключей шифрования между пользователями.

Перед началом обмена зашифрованными данными необходимо обменяться секретными ключами со всеми адресатами. Передача секретного ключа симметричной криптосистемы не может быть осуществлена по общедоступным каналам связи, секретный ключ надо передавать отправителю и получателю по защищенному каналу.

Существуют реализации алгоритмов симметричного шифрования для абонентского шифрования данных — т. е. для отправки шифрованной информации абоненту, например, через Интернет. Использование одного ключа для всех абонентов подобной криптографической сети недопустимо по соображениям безопасности. Действительно, в случае компрометации (утери, хищения) ключа под угрозой будет находиться документооборот всех абонентов. В этом случае может быть использована матрица ключей (рис. 4.4).

	1	2	3	...	n	
1	K_{11}	K_{12}	K_{13}	...	K_{1n}	Набор ключей для абонента 1
2	K_{21}	K_{22}	K_{23}	...	K_{2n}	Набор ключей для абонента 2
3	K_{31}	K_{32}	K_{33}	...	K_{3n}	Набор ключей для абонента 3
...	...	...	...	...	...	...
n	K_{n1}	K_{n2}	K_{n3}	...	K_{nn}	Набор ключей для абонента n

Рис. 4.4. Матрица ключей

Матрица ключей представляет собой таблицу, содержащую ключи парной связи абонентов. Каждый элемент таблицы K_{ij} предназначен для

связи абонентов i и j и доступен только двум данным абонентам. Соответственно, для всех элементов матрицы ключей соблюдается равенство

$$K_{ij} = K_{ji}.$$

Каждая i-я строка матрицы представляет собой набор ключей конкретного абонента i для связи с остальными $N - 1$ абонентами. Наборы ключей (сетевые наборы) распределяются между всеми абонентами криптографической сети. Аналогично сказанному выше, сетевые наборы должны распределяться *по защищенным каналам* связи или из рук в руки. Методы, обеспечивающие защищенное распределение ключей абонентам сети, рассматриваются в разделе 4.6.

Характерной особенностью симметричных криптоалгоритмов является то, что в ходе своей работы они производят преобразование блока входной информации фиксированной длины и получают результирующий блок того же объема, но недоступный для прочтения сторонним лицам, не владеющим ключом. Схему работы симметричного блочного шифра можно описать функциями

$$C = E_K(M) \text{ и } M = D_K(C),$$

где M — исходный (открытый) блок данных; C — зашифрованный блок данных.

Ключ K является параметром симметричного блочного криптоалгоритма и представляет собой блок двоичной информации фиксированного размера. Исходный M и зашифрованный C блоки данных также имеют фиксированную разрядность, равную между собой, но необязательно равную длине ключа K.

Блочные шифры являются той основой, на которой реализованы практически все симметричные криптосистемы. Симметричные криптосистемы позволяют кодировать и декодировать файлы произвольной длины. Практически все алгоритмы используют для преобразований определенный набор обратимых математических преобразований.

Методика создания цепочек из зашифрованных блочными алгоритмами байтов позволяет шифровать ими пакеты информации неограниченной длины. Отсутствие статистической корреляции между битами выходного потока блочного шифра используется для вычисления контрольных сумм пакетов данных и в хэшировании паролей. На сегодняшний день разработано достаточно много стойких блочных шифров.

Криптоалгоритм считается идеально стойким, если для прочтения зашифрованного блока данных необходим перебор всех возможных ключей до тех пор, пока расшифрованное сообщение не окажется осмысленным. В общем случае стойкость блочного шифра зависит только от длины ключа и возрастает экспоненциально с ее ростом.

К. Шеннон предложил для получения стойких блочных шифров использовать два общих принципа: рассеивание и перемешивание [7].

Рассеивание представляет собой распространение влияния одного знака открытого текста на много знаков шифртекста, что позволяет скрыть статистические свойства открытого текста.

Перемешивание предполагает использование таких шифрующих преобразований, которые усложняют восстановление взаимосвязи статистических свойств открытого и шифрованного текстов. Однако шифр должен не только затруднять раскрытие, но и обеспечивать легкость зашифрования и расшифрования при известном пользователю секретном ключе.

Распространенным способом достижения эффектов рассеивания и перемешивания является использование составного шифра, т. е. такого, который может быть реализован в виде некоторой последовательности простых шифров, каждый из которых вносит свой вклад в значительное суммарное рассеивание и перемешивание.

В составных шифрах в качестве простых шифров чаще всего используются простые перестановки и подстановки. При перестановке просто перемешивают символы открытого текста, причем конкретный вид перемешивания определяется секретным ключом. При подстановке каждый символ открытого текста заменяют другим символом из того же алфавита, а конкретный вид подстановки также определяется секретным ключом. Следует заметить, что в современном блочном шифре блоки открытого текста и шифртекста представляют собой двоичные последовательности обычно длиной 64 или 128 бит. При длине 64 бит каждый блок может принимать 2^{64} значений. Поэтому подстановки выполняются в очень большом алфавите, содержащем до $2^{64} \approx 10^{19}$ «символов».

При многократном чередовании простых перестановок и подстановок, управляемых достаточно длинным секретным ключом, можно получить стойкий шифр с хорошим рассеиванием и перемешиванием.

Все действия, производимые блочным криптоалгоритмом над данными, основаны на том факте, что преобразуемый блок может быть представлен в виде целого неотрицательного числа из диапазона, соответствующего его разрядности. Например, 32-битный блок данных можно интерпретировать как число из диапазона 0...4 294 967 295. Кроме того, блок, разрядность которого представляет собой «степень двойки», можно трактовать как сцепление нескольких независимых неотрицательных чисел из меньшего диапазона (указанный выше 32-битный блок можно также представить в виде сцепления двух независимых 16-битных чисел из диапазона 0...65 535 или в виде сцепления четырех независимых 8-битных чисел из диапазона 0...255).

Над этими числами блочный криптоалгоритм производит по определенной схеме действия, перечисленные в табл. 4.1.

В качестве параметра V для любого из этих преобразований может использоваться:

- фиксированное число (например, $X' = X + 125$);
- число, получаемое из ключа (например, $X' = X + F(K)$);
- число, получаемое из независимой части блока (например, $X2' = X2 + F(X1)$).

Последний вариант используется в схеме, называемой сетью Фейстеля (по имени ее создателя).

Таблица 4.1. **Действия, выполняемые криптоалгоритмом над числами**

Действие	Функция
Математические функции	
Сложение	$X' = X + V$
Исключающее ИЛИ	$X' = X$ XOR V
Умножение по модулю $(2N + 1)$	$X' = (X * V) \bmod (2N + 1)$
Умножение по модулю $2N$	$X' = (X * V) \bmod (2N)$
Битные сдвиги	
Арифметический сдвиг влево	$X' = X$ SHL V
Арифметический сдвиг вправо	$X' = X$ SHR V
Циклический сдвиг влево	$X' = X$ ROL V
Циклический сдвиг вправо	$X' = X$ ROR V
Табличные подстановки	
S-box (substitute)	X' = Table $[X, V]$

Последовательность выполняемых над блоком операций, комбинации перечисленных выше вариантов V и сами функции F и составляют отличительные особенности конкретного симметричного блочного криптоалгоритма.

Характерным признаком блочных алгоритмов является многократное и косвенное использование материала ключа. Это определяется в первую очередь требованием невозможности обратного декодирования в отношении ключа при известных исходном и зашифрованном текстах. Для решения этой задачи в приведенных выше преобразованиях чаще всего используется не само значение ключа или его части, а некоторая, иногда необратимая функция от материала ключа. Более того, в подобных преобразованиях один и тот же блок или элемент ключа используется многократно. Это позволяет при выполнении условия обратимости функции относительно величины X сделать функцию необратимой относительно ключа K [83].

4.2.1. Алгоритмы шифрования DES и 3-DES

Алгоритм шифрования данных DES (Data Encryption Standard) был опубликован в 1977 г. Блочный симметричный алгоритм DES остается пока распространенным алгоритмом, используемым в системах защиты коммерческой информации.

Алгоритм DES построен в соответствии с методологией сети Фейстеля и состоит из чередующейся последовательности перестановок и подстановок. Алгоритм DES осуществляет шифрование 64-битных бло-

ков данных с помощью 64-битного ключа, в котором значащими являются 56 бит (остальные 8 бит — проверочные биты для контроля на четность). Обобщенная схема процесса шифрования в блочном алгоритме DES показана на рис. 4.5.

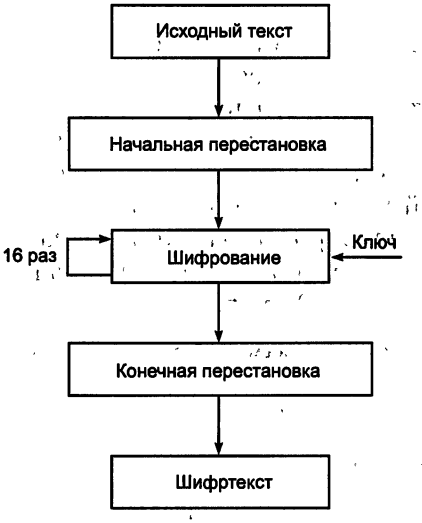


Рис. 4.5. Обобщенная схема шифрования в алгоритме DES

Процесс шифрования заключается в начальной перестановке битов 64-битного блока, шестнадцати циклах (раундах) шифрования и, наконец, в конечной перестановке битов.

Расшифрование в DES является операцией, обратной шифрованию, и выполняется путем повторения операций шифрования в обратной последовательности.

Основные достоинства алгоритма DES:

- используется только один ключ длиной 56 бит;
- относительная простота алгоритма обеспечивает высокую скорость обработки;
- зашифровав сообщение с помощью одного пакета программ, для расшифровки можно использовать любой другой пакет программ, соответствующий алгоритму DES;
- криптостойкость алгоритма вполне достаточна для обеспечения информационной безопасности большинства коммерческих приложений.

Современная микропроцессорная техника позволяет уже сегодня за достаточно приемлемое время взламывать симметричные блочные шифры с длиной ключа 40 бит. Для такого взламывания используется метод полного перебора — тотального опробования всех возможных значений ключа (метод «грубой силы»).

До недавнего времени блочный алгоритм DES, имеющий ключ с эффективной длиной 56 бит, считался относительно безопасным алгоритмом шифрования. Он многократно подвергался тщательному крип-

тоанализу в течение 20 лет, и самым практичным способом его взламывания является метод перебора всех возможных значений ключа. Ключ шифра DES имеет 2^{56} возможных значений.

В настоящее время на рынке имеются FPGA-чипы, обладающие возможностью перебирать до 30 миллионов значений ключа в секунду. Еще бо́льшие возможности имеют ASIC-чипы — они реализуют скорость перебора до 200 миллионов ключей в секунду. Стоимость этих чипов составляет всего лишь десятки долларов. Поэтому вполне актуальны оценки криптостойкости шифра DES, включающие ориентировочные расчеты времени и материальных средств, которые необходимо затратить на взламывание этого шифра методом полного перебора всех возможных значений ключа с использованием как стандартных компьютеров, так и специализированных криптоаналитических аппаратных средств. В табл. 4.2 приведены результаты анализа трудоемкости взламывания криптоалгоритма DES [63].

Таблица 4.2. **Сравнительный анализ трудоемкости взлома криптоалгоритма DES**

Тип атакующего	Бюджет атакующего	Средства атаки	Затраты времени на успешную атаку
Хакер	До 500 долл.	ПК	Несколько десятков лет
Небольшие фирмы	До 10 тыс. долларов	FPGA	18 месяцев
Корпоративные департаменты	До 300 тыс. долл.	FPGA ASIC	19 дней 3 дня
Большие корпорации	До 10 млн долл.	FPGA, ASIC Супер-ЭВМ	13 ч 6 мин
Специальные агентства	?	?	?

Возникает естественный вопрос: нельзя ли использовать DES в качестве строительного блока для создания другого алгоритма с более длинным ключом?

Комбинирование блочных алгоритмов

В принципе, существует много способов комбинирования блочных алгоритмов для получения новых алгоритмов. Одним из таких способов комбинирования является многократное шифрование, т. е. использование блочного алгоритма несколько раз с разными ключами для шифрования одного и того же блока открытого текста.

У. Тачмен предложил шифровать блок открытого текста P три раза с помощью двух ключей K_1 и K_2 (рис. 4.6) [63]. Процедура шифрования:

$$C = E_{K1}(D_{K2}(E_{K1}(P))),$$

т. е. блок открытого текста P сначала шифруется ключом K_1, затем расшифровывается ключом K_2 и окончательно зашифровывается ключом K_1.

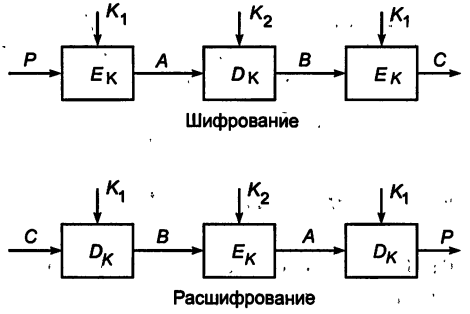


Рис. 4.6. Схемы трехкратного применения блочного алгоритма симметричного шифрования с двумя различными ключами

Этот режим иногда называют режимом EDE (Encrypt-Decrypt-Encrypt). Введение в данную схему операции расшифрования D_{K2} позволяет обеспечить совместимость этой схемой со схемой однократного использования блочного алгоритма DES. Если в схеме трехкратного использования DES выбрать все ключи одинаковыми, то эта схема превращается в схему однократного использования DES. Процедура расшифрования выполняется в обратном порядке:

$$P = D_{K1}(E_{K2}(D_{K1}(C))),$$

т. е. блок шифртекста C сначала расшифровывается ключом K_1, затем зашифровывается ключом K_2 и окончательно расшифровывается ключом K_1.

Если исходный блочный алгоритм имеет n-битный ключ, то схема трехкратного шифрования имеет $2n$-битный ключ. Чередование ключей K_1 и K_2 позволяет предотвратить криптоаналитическую атаку «человек-в-середине». Данная схема приводится в стандартах X9.17 и ISO 8732 в качестве средства улучшения характеристик алгоритма DES.

При трехкратном шифровании можно применить три различных ключа. При этом возрастает общая длина результирующего ключа. Процедуры шифрования и расшифрования описываются следующими выражениями:

$$C = E_{K3}(D_{K2}(E_{K1}(P))),$$

$$P = D_{K1}(E_{K2}(D_{K3}(C))).$$

Трехключевой вариант имеет еще бо́льшую стойкость. Алгоритм 3-DES (Triple DES — тройной DES) используется в ситуациях, когда надежность алгоритма DES считается недостаточной. Чаще всего используется вариант шифрования на трех ключах: открытый текст шифруется на первом ключе, полученный шифртекст — на втором ключе, и наконец, данные, полученные после второго шага, шифруются на третьем ключе. Все три ключа выбираются независимо друг от друга. Этот криптоалгоритм достаточно стоек ко всем атакам. Применяется также каскадный вариант 3-DES. Это стандартный тройной DES, к которому добавлен такой механизм обратной связи, как CBC, OFB или CFB.

Сегодня все шире используются два современных криптостойких алгоритма шифрования: отечественный стандарт шифрования ГОСТ 28147—89 и новый криптостандарт США — AES (Advanced Encryption Standard).

4.2.2. Стандарт шифрования ГОСТ 28147—89

Этот алгоритм криптографического преобразования данных предназначен для аппаратной и программной реализации, удовлетворяет криптографическим требованиям и не накладывает ограничений на степень секретности защищаемой информации. Алгоритм шифрования данных, определяемый ГОСТ 28147—89, представляет собой 64-битный блочный алгоритм с 256-битным ключом.

Данные, подлежащие зашифрованию, разбивают на 64-разрядные блоки. Эти блоки разбиваются на два субблока N_1 и N_2 по 32 бит (рис. 4.7).

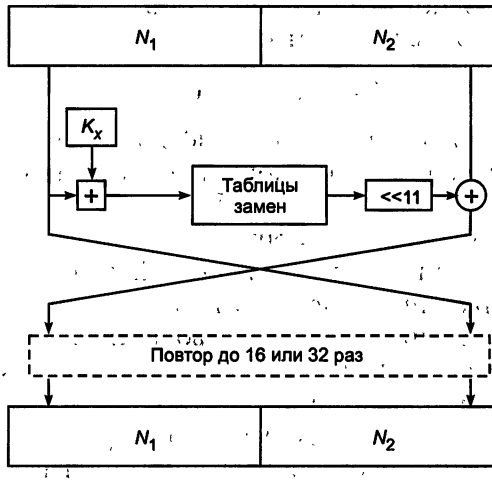


Рис. 4.7. Схема алгоритма ГОСТ 28147—89

Субблок N_1 обрабатывается определенным образом, после чего его значение складывается со значением субблока N_2 (сложение выполняется по модулю 2, т. е. применяется логическая операция XOR — исключающее ИЛИ), а затем субблоки меняются местами. Данное преобразование выполняется определенное число раз (раундов): 16 или 32 в зависимости от режима работы алгоритма.

В каждом раунде выполняются две операции.

Первая операция — наложение ключа. Содержимое субблока N_1 складывается по модулю 2^{32} с 32-битной частью ключа K_x. Полный ключ шифрования представляется в виде конкатенации 32-битных подключей: K_0, K_1, K_2, K_3, K_4, K_5, K_6, K_7. В процессе шифрования используется один из этих подключей — в зависимости от номера раунда и режима работы алгоритма.

Вторая операция — табличная замена. После наложения ключа субблок $N1$ разбивается на 8 частей по 4 бит, значение каждой из которых заменяется в соответствии с таблицей замены для данной части субблока. Затем выполняется побитный циклический сдвиг субблока влево на 11 бит.

Табличные замены. Блок подстановки S-box (Substitution box) часто используют в современных алгоритмах шифрования, поэтому стоит пояснить, как организуется подобная операция.

Блок подстановки S-box состоит из восьми узлов замены (*S*-блоков замены) S_1, S_2, ..., S_8 с памятью 64 бит каждый. Поступающий на блок подстановки S 32-битный вектор разбивают на восемь последовательно идущих 4-битных векторов, каждый из которых преобразуется в 4-битный вектор соответствующим узлом замены. Каждый узел замены можно представить в виде таблицы-перестановки шестнадцати 4-битных двоичных чисел в диапазоне 0000...1111. Входной вектор указывает адрес строки в таблице, а число в этой строке является выходным вектором. Затем 4-битные выходные векторы последовательно объединяют в 32-битный вектор. Узлы замены (таблицы-перестановки) представляют собой ключевые элементы, которые являются общими для сети ЭВМ и редко изменяются. Эти узлы замены должны сохраняться в секрете.

Алгоритм, определяемый ГОСТ 28147—89, предусматривает четыре режима работы: простой замены, гаммирования, гаммирования с обратной связью и генерации имитовставок. В них используется одно и то же описанное выше шифрующее преобразование, но, поскольку назначение режимов различно, осуществляется это преобразование в каждом из них по-разному.

В режиме *простой замены* для зашифрования каждого 64-битного блока информации выполняются 32 описанных выше раунда. При этом 32-битные подключи используются в следующей последовательности:

- K_0, K_1, K_2, K_3, K_4, K_5, K_6, K_7, K_0, K_1 и т. д. — в раундах с 1-го по 24-й;
- K_7, K_6, K_5, K_4, K_3, K_2, K_1, K_0 — в раундах с 25-го по 32-й.

Расшифрование в данном режиме проводится точно так же, но с несколько другой последовательностью применения подключей:

- K_0, K_1, K_2, K_3, K_4, K_5, K_6, K_7 — в раундах с 1-го по 8-й;
- K_7, K_6, K_5, K_4, K_3, K_2, K_1, K_0, K_7, K_6 и т. д. — в раундах с 9-го по 32-й.

Все блоки шифруются независимо друг от друга, т. е. результат зашифрования каждого блока зависит только от его содержимого (соответствующего блока исходного текста). При наличии нескольких одинаковых блоков исходного (открытого) текста соответствующие им блоки шифртекста тоже будут одинаковы, что дает дополнительную полезную информацию для пытающегося вскрыть шифр криптоаналитика. Поэтому данный режим применяется в основном для шифрования самих ключей шифрования (очень часто реализуются многоключевые схемы, в

которых по ряду соображений ключи шифруются друг на друге). Для шифрования собственно информации предназначены два других режима работы — гаммирования и гаммирования с обратной связью.

В *режиме гаммирования* каждый блок открытого текста побитно складывается по модулю 2 с блоком гаммы шифра размером 64 бит. *Гамма шифра* — это специальная последовательность, которая получается в результате определенных операций с регистрами N_1 и N_2 (рис. 4.8).

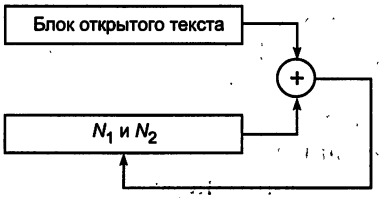


Рис. 4.8. Выработка гаммы шифра в режиме гаммирования с обратной связью

1. В регистры N_1 и N_2 записывается их начальное заполнение — 64-битная величина, называемая синхропосылкой.
2. Выполняется зашифрование содержимого регистров N_1 и N_2 (в данном случае синхропосылки) в режиме простой замены.
3. Содержимое регистра N_1 складывается по модулю $(2^{32} - 1)$ с константой $C_1 = 2^{24} + 2^{16} + 2^8 + 2^4$, а результат сложения записывается в регистр N_1.
4. Содержимое регистра N_2 складывается по модулю 2^{32} с константой $C_2 = 2^{24} + 2^{16} + 2^8 + 1$, а результат сложения записывается в регистр N_2.
5. Содержимое регистров N_1 и N_2 подается на выход в качестве 64-битного блока гаммы шифра (в данном случае N_1 и N_2 образуют первый блок гаммы).

Если необходим следующий блок гаммы (т. е. необходимо продолжить зашифрование или расшифрование), выполняется возврат к операции 2.

Для расшифрования гамма вырабатывается аналогичным образом, а затем к битам зашифрованного текста и гаммы снова применяется операция XOR. Поскольку эта операция обратима, в случае правильно выработанной гаммы получается исходный текст (табл. 4.3).

Таблица 4.3. **Зашифрование и расшифрование в режиме гаммирования**

	Операция	Результат
Исходный текст		100100
Гамма	XOR	111000
Шифртекст	=	011100
Гамма	XOR	111000
Исходный текст	=	100100

Для выработки нужной для расшифровки гаммы шифра у пользователя, расшифровывающего криптограмму, должен быть тот же ключ и то же значение синхропосылки, которые применялись при зашифровании информации. В противном случае получить исходный текст из зашифрованного не удастся.

В большинстве реализаций алгоритма ГОСТ 28147—89 синхропосылка не секретна, однако есть системы, где синхропосылка — такой же секретный элемент, как и ключ шифрования. Для таких систем эффективная длина ключа алгоритма (256 бит) увеличивается еще на 64 бит секретной синхропосылки, которую также можно рассматривать как ключевой элемент.

В *режиме гаммирования с обратной связью* для заполнения регистров N_1 и N_2, начиная со 2-го блока, используется не предыдущий блок гаммы, а результат зашифрования предыдущего блока открытого текста (см. рис. 4.8). Первый же блок в данном режиме генерируется полностью аналогично предыдущему.

Рассматривая режим *генерации имитовставок*, следует определить понятие предмета генерации. Имитовставка — это криптографическая контрольная сумма, вычисляемая с использованием ключа шифрования и предназначенная для проверки целостности сообщений. При генерации имитовставки выполняются следующие операции: первый 64-битный блок массива информации, для которого вычисляется имитовставка, записывается в регистры N_1 и N_2 и зашифровывается в сокращенном режиме простой замены (выполняются первые 16 раундов из 32). Полученный результат суммируется по модулю 2 со следующим блоком информации с сохранением результата в N_1 и N_2.

Цикл повторяется до последнего блока информации. Получившееся в результате этих преобразований 64-битное содержимое регистров N_1 и N_2 или его часть и называется имитовставкой. Размер имитовставки выбирается, исходя из требуемой достоверности сообщений: при длине имитовставки r бит вероятность, что изменение сообщения останется незамеченным, равна 2^{-r}.

Чаще всего используется 32-битная имитовставка, т. е. половина содержимого регистров. Этого достаточно, поскольку, как любая контрольная сумма, имитовставка предназначена прежде всего для защиты от случайных искажений информации. Для защиты же от преднамеренной модификации данных применяются другие криптографические методы — в первую очередь электронная цифровая подпись.

При обмене информацией имитовставка служит своего рода дополнительным средством контроля. Она вычисляется для открытого текста при зашифровании какой-либо информации и посылается вместе с шифртекстом. После расшифрования вычисляется новое значение имитовставки, которое сравнивается с присланной. Если значения не совпадают, значит, шифртекст был искажен при передаче или при расшифровании использовались неверные ключи. Особенно полезна имитовставка для проверки правильности расшифрования ключевой информации при использовании многоключевых схем.

Алгоритм ГОСТ 28147—89 считается очень стойким — в настоящее время для его раскрытия не предложено более эффективных методов, чем упомянутый выше метод «грубой силы». Его высокая стойкость достигается в первую очередь за счет большой длины ключа — 256 бит. При использовании секретной синхропосылки эффективная длина ключа увеличивается до 320 бит, а засекречивание таблицы замен прибавляет дополнительные биты. Кроме того, криптостойкость зависит от количества раундов преобразований, которых по ГОСТ 28147—89 должно быть 32 (полный эффект рассеивания входных данных достигается уже после 8 раундов).

4.2.3. Американский стандарт шифрования AES

В 1997 г. Американский институт стандартизации NIST (National Institute of Standards & Technology) объявил конкурс на новый стандарт симметричного криптоалгоритма, названного AES (Advanced Encryption Standard). К его разработке были подключены самые крупные центры криптологии со всего мира.

К криптоалгоритмам — кандидатам на новый стандарт AES были предъявлены следующие требования:

- алгоритм должен быть симметричным;
- алгоритм должен быть блочным шифром;
- алгоритм должен иметь длину блока 128 бит и поддерживать три длины ключа: 128, 192 и 256 бит.

Дополнительно разработчикам криптоалгоритмов рекомендовалось:

- использовать операции, легко реализуемые как аппаратно (в микрочипах), так и программно (на персональных компьютерах и серверах);
- ориентироваться на 32-разрядные процессоры;
- не усложнять без необходимости структуру шифра, для того чтобы все заинтересованные стороны были в состоянии самостоятельно провести независимый криптоанализ алгоритма и убедиться, что в нем не заложено каких-либо недокументированных возможностей.

На этот конкурс было представлено 15 алгоритмов-претендентов, разработанных как известными в области криптографии организациями (RSA Security, Counterpane и т. д.), так и частными лицами. Итоги конкурса были подведены в октябре 2000 г.: победителем был объявлен алгоритм Rijndael, разработанный двумя криптографами из Бельгии, Винсентом Риджменом (Vincent Rijmen) и Джоан Даймен (Joan Daemen). Алгоритм Rijndael стал новым стандартом шифрования данных AES [97].

Алгоритм AES не похож на большинство известных алгоритмов симметричного шифрования, структура которых носит название «сеть Фейстеля» и аналогична российскому ГОСТ 28147—89. В отличие от отечественного стандарта шифрования, алгоритм AES представляет каждый блок обрабатываемых данных в виде двухмерного байтного массива раз-

мером 4 × 4, 4 × 6 или 4 × 8 в зависимости от установленной длины блока (допускается использование нескольких фиксированных размеров шифруемого блока информации). Далее на соответствующих этапах производятся преобразования либо над независимыми столбцами, либо над независимыми строками, либо вообще над отдельными байтами.

Алгоритм AES состоит из определенного количества раундов (от 10 до 14 — это зависит от размера блока и длины ключа) и выполняет четыре преобразования:

- BS (`ByteSub`) — табличная замена каждого байта массива (рис. 4.9);
- SR (`ShiftRow`) — сдвиг строк массива (рис. 4.10). При этой операции первая строка остается без изменений, а остальные циклически побайтно сдвигаются влево на фиксированное число байтов, зависящее от размера массива. Например, для массива размером 4 × 4 строки 2, 3 и 4 сдвигаются соответственно на 1, 2 и 3 байта;
- MC (`MixColumn`) — операция над независимыми столбцами массива (рис. 4.11), когда каждый столбец по определенному правилу умножается на фиксированную матрицу $c(x)$;

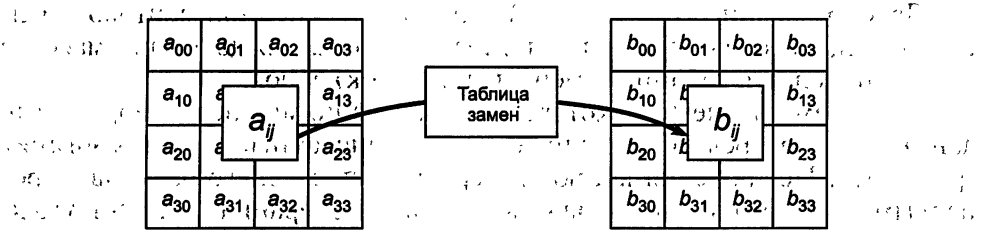


Рис. 4.9. Преобразование BS (`ByteSub`) использует таблицу замен (подстановок) для обработки каждого байта массива `State`

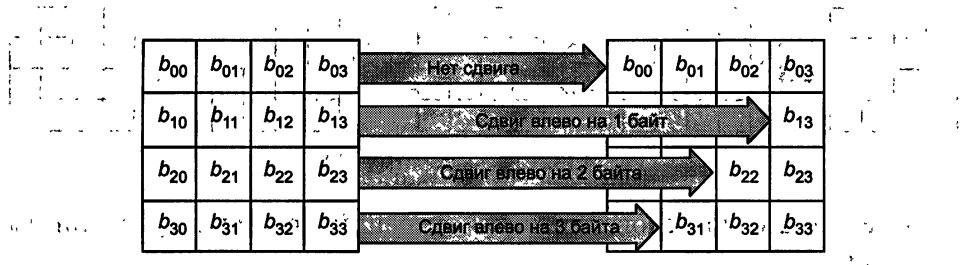


Рис. 4.10. Преобразование SR (`ShiftRow`) циклически сдвигает три последние строки в массиве `State`

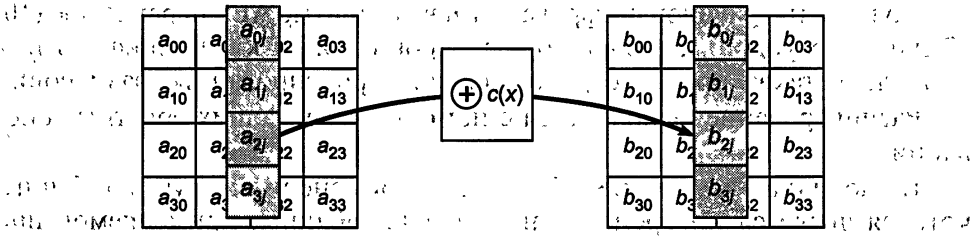


Рис. 4.11. Преобразование MC (`MixColumn`) поочередно обрабатывает столбцы массива `State`

- AK (AddRoundKey) — добавление ключа. Каждый бит массива складывается по модулю 2 с соответствующим битом ключа раунда, который, в свою очередь, определенным образом вычисляется из ключа шифрования (рис. 4.12).

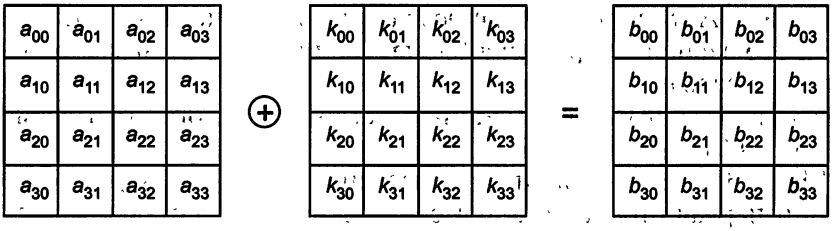


Рис. 4.12. Преобразование AK (AddRoundKey) производит сложение XOR каждого столбца массива State со словом из ключевого набора

Эти преобразования воздействуют на массив State, который адресуется с помощью указателя 'state'. Преобразование AddRoundKey использует дополнительный указатель для адресации ключа раунда RoundKey.

Преобразование BS (ByteSub) является нелинейной байтовой подстановкой, которая воздействует независимо на каждый байт массива State, используя таблицу замен (подстановок) S-box.

В каждом раунде (с некоторыми исключениями) над шифруемыми данными поочередно выполняются перечисленные преобразования (рис. 4.13). Исключения касаются первого и последнего раундов: перед первым раундом дополнительно выполняется операция AK, а в последнем раунде отсутствует MC.

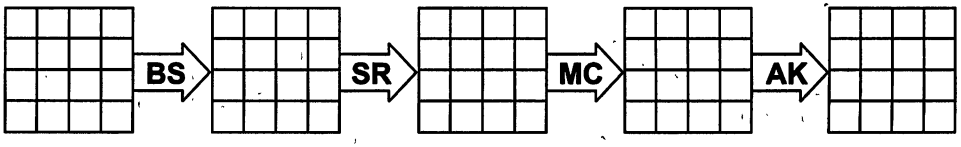


Рис. 4.13. Раунд алгоритма AES

В результате последовательность операций при зашифровании выглядит так:

AK, {BS, SR, MC, AK} (повторяется $R-1$ раз), BS, SR, AK.

Количество раундов шифрования R в алгоритме AES переменное (10, 12 или 14 раундов) и зависит от размеров блока и ключа шифрования (для ключа также предусмотрено несколько фиксированных размеров).

Расшифрование выполняется с помощью следующих обратных операций.

1. Табличная замена BS обращается применением другой таблицы, которая является инверсной относительно таблицы, применяемой при зашифровании.

2. Обратной операцией к SR является циклический сдвиг строк вправо, а не влево.

3. Обратная операция для MC — умножение по тем же правилам на другую матрицу $d(x)$, удовлетворяющую условию $c(x) \cdot d(x) = 1$.

4. Добавление ключа AK является обратным самому себе, поскольку в нем используется только операция XOR.

Эти обратные операции применяются при расшифровании в последовательности, обратной той, что использовалась при зашифровании.

Все преобразования в шифре AES имеют строгое математическое обоснование. Сама структура и последовательность операций позволяют выполнять данный алгоритм эффективно как на 8-, так и на 32-битных процессорах. В структуре алгоритма заложена возможность параллельного исполнения некоторых операций, что может поднять скорость шифрования на многопроцессорных рабочих станциях в 4 раза.

Алгоритм Rijndael стал новым стандартом шифрования данных AES благодаря целому ряду преимуществ перед другими алгоритмами. Прежде всего, он обеспечивает высокую скорость шифрования на всех платформах: как при программной, так и при аппаратной реализации. Кроме того, требования к ресурсам для его работы минимальны, что важно при его использовании в устройствах, обладающих ограниченными вычислительными возможностями.

Недостатком же алгоритма AES можно считать лишь свойственную ему нетрадиционную схему. Дело в том, что свойства алгоритмов, основанных на сети Фейстеля, хорошо исследованы, а AES, в отличие от них, может содержать скрытые уязвимости, которые могут обнаружиться только по прошествии какого-то времени с момента начала его широкого распространения.

Другие симметричные криптоалгоритмы

Для шифрования данных применяются и другие блочные симметричные криптоалгоритмы.

Алгоритм IDEA (International Data Encryption Algorithm) — еще один 64-битный блочный шифр с длиной ключа 128 бит. Этот европейский стандарт криптоалгоритма предложен в 1990 г. Алгоритм IDEA по скорости не уступает алгоритму DES, а по стойкости к криптоанализу превосходит DES.

Алгоритм RC2 представляет собой 64-битный блочный шифр с ключом переменной длины. Этот алгоритм приблизительно в 2 раза быстрее, чем DES. Может использоваться в тех же режимах, что и DES, включая тройное шифрование. Владельцем алгоритма является компания RSA Data Security.

Алгоритм RC5 представляет собой быстрый блочный шифр, который имеет размер блока 32, 64 или 128 бит, ключ длиной от 0 до 2048 бит. Алгоритм выполняет от 0 до 255 проходов. Алгоритмом владеет компания RSA Data Security.

Алгоритм Blowfish — это 64-битный блочный шифр, имеет ключ переменного размера до 448 бит, выполняет 16 проходов, на каждом проходе осуществляются перестановки, зависящие от ключа, и подстановки, зависящие от ключа и данных. Этот алгоритм быстрее алгоритма DES.

4.2.4. Основные режимы работы блочного симметричного алгоритма

Рассмотрим основные режимы работы блочного симметричного алгоритма. Большинство блочных симметричных криптоалгоритмов непосредственно преобразуют 64-битный входной открытый текст в 64-битный выходной шифрованный текст, однако данные редко ограничиваются 64 разрядами.

Чтобы воспользоваться блочным симметричным алгоритмом для решения разнообразных криптографических задач, разработано четыре рабочих режима:

- электронная кодовая книга ECB (Electronic Code Book);
- сцепление блоков шифра CBC (Cipher Block Chaining);
- обратная связь по шифртексту CFB (Cipher Feed Back);
- обратная связь по выходу OFB (Output Feed Back).

Эти рабочие режимы первоначально были разработаны для блочного алгоритма DES, но в любом из этих режимов могут работать и другие блочные криптоалгоритмы. В качестве примера будем использовать блочный алгоритм DES.

Режим «Электронная кодовая книга»

Длинный файл разбивают на 64-битные отрезки (блоки) по 8 байт. Каждый из этих блоков шифруют независимо с использованием одного и того же ключа шифрования (рис. 4.14).

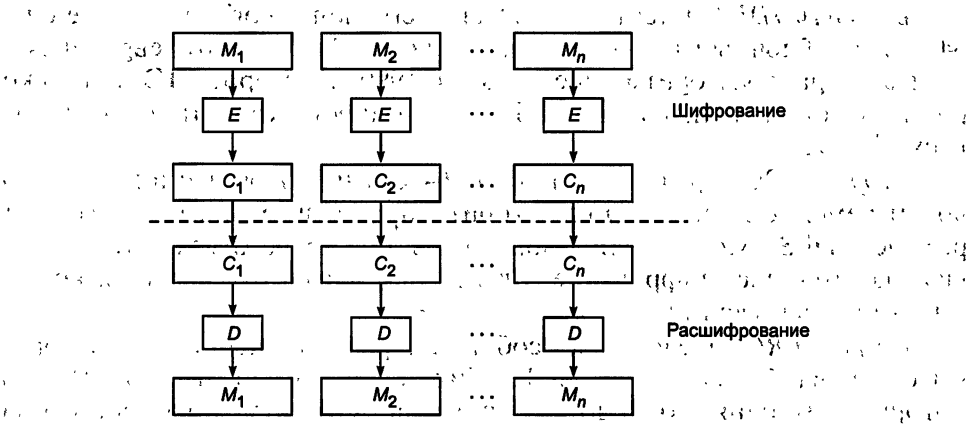


Рис. 4.14. Схема работы блочного алгоритма в режиме электронной кодовой книги

Основное достоинство — простота реализации. Недостаток — относительно слабая устойчивость против криптоаналитических атак. Из-за фиксированного характера шифрования при ограниченной длине блока 64 бит возможно проведение криптоанализа со словарем. Блок такого размера может повториться в сообщении вследствие большой избыточности в тексте на естественном языке. Это приводит к тому, что идентичные блоки открытого текста в сообщении будут представлены идентичными блоками шифртекста, что дает криптоаналитику некоторую информацию о содержании сообщения.

Режим «Сцепление блоков шифра»

В этом режиме исходный файл M разбивается на 64-битные блоки: $M = M_1 M_2 \ldots M_n$. Первый блок M_1 складывается по модулю 2 с 64-битным начальным вектором IV, который меняется ежедневно и держится в секрете (рис. 4.15).

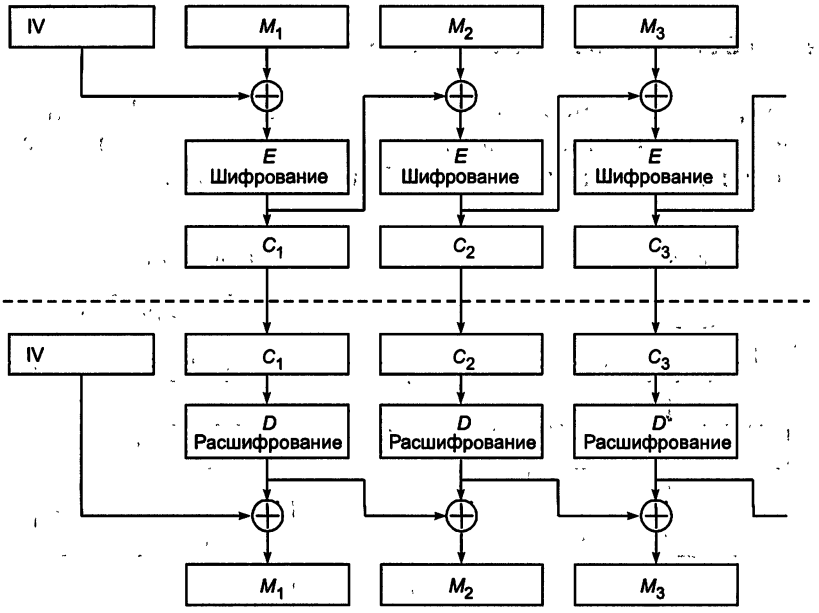


Рис. 4.15. Схема работы блочного алгоритма в режиме сцепления блоков шифра

Полученная сумма затем шифруется с использованием ключа шифра, известного и отправителю, и получателю информации. Полученный 64-битный блок шифртекста C_1 складывается по модулю 2 со вторым блоком текста, результат шифруется и получается второй 64-битный блок шифртекста C_2 и т. д. Процедура повторяется до тех пор, пока не будут обработаны все блоки текста.

Таким образом, для всех $i = 1 \ldots n$ (n — число блоков) результат шифрования C_i определяется следующим образом: $C_i = E(M_i \oplus C_{i-1})$, где

C_0 = IV — начальное значение шифра, равное начальному вектору (вектору инициализации).

Очевидно, что последний 64-битный блок шифртекста является функцией секретного ключа, начального вектора и каждого бита открытого текста независимо от его длины. Этот блок шифртекста называют *кодом аутентификации сообщения MAC* (Message Authentication Code).

Код MAC может быть легко проверен получателем, владеющим секретным ключом и начальным вектором, путем повторения процедуры, выполненной отправителем. Посторонний, однако, не может осуществить генерацию MAC, который воспринялся бы получателем как подлинный, чтобы добавить его к ложному сообщению, либо отделить MAC от истинного сообщения для использования его с измененным или ложным сообщением. Достоинство данного режима в том, что он не позволяет накапливаться ошибкам при передаче.

Блок M_i является функцией только C_{i-1} и C_i. Поэтому ошибка при передаче приведет к потере только двух блоков исходного текста.

Режим «Обратная связь по шифртексту»

В этом режиме размер блока может отличаться от 64 бит (рис. 4.16). Файл, подлежащий шифрованию (расшифрованию), считывается последовательными блоками длиной k битов (k = 1...64).

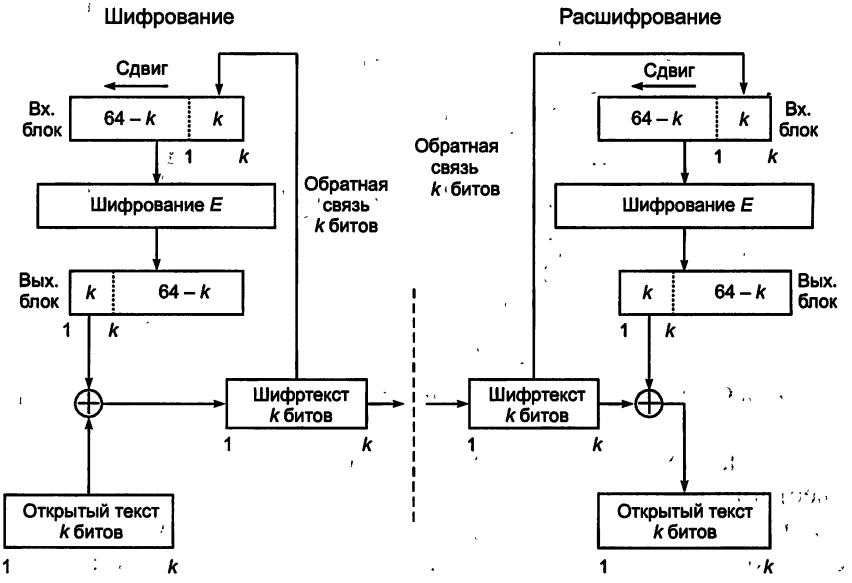


Рис. 4.16. Схема работы блочного алгоритма в режиме обратной связи по шифртексту

Входной блок (64-битный регистр сдвига) вначале содержит вектор инициализации, выровненный по правому краю.

Предположим, что в результате разбиения на блоки мы получили n блоков длиной k битов каждый (остаток дописывается нулями или пробелами). Тогда для любого $i = 1...n$ блок шифртекста $C_i = M_i \oplus P_{i-1}$, где P_{i-1} обозначает k старших битов предыдущего зашифрованного блока.

Обновление сдвигового регистра осуществляется путем удаления его старших k битов и записи C_i в регистр. Восстановление зашифрованных данных выполняют относительно просто: P_{i-1} и C_i вычисляются аналогичным образом и $M_i = C_i \oplus P_{i-1}$.

Режим «Обратная связь по выходу»

Этот режим тоже использует переменный размер блока и сдвиговый регистр, инициализируемый так же, как в режиме CFB, а именно входной блок вначале содержит вектор инициализации IV, выровненный по правому краю (рис. 4.17).

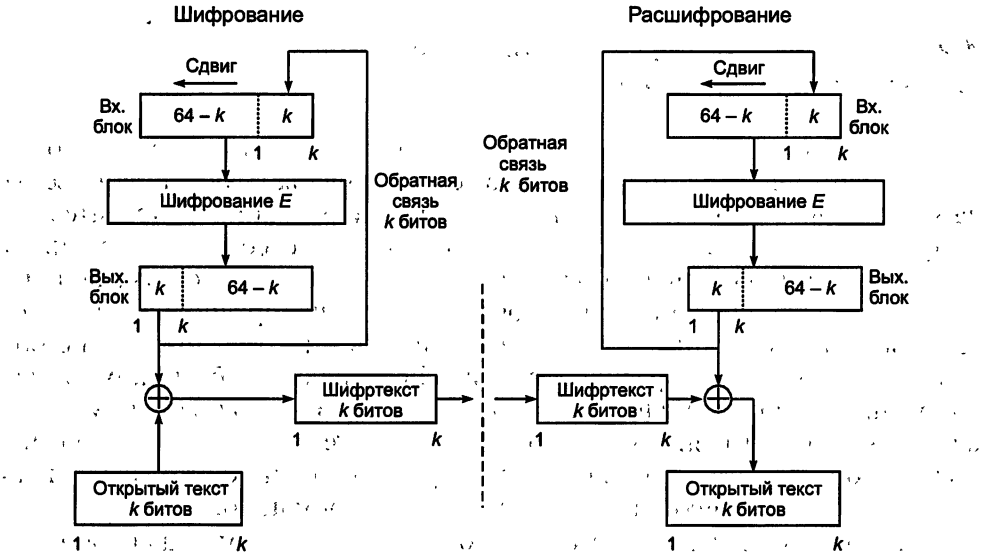


Рис. 4.17. Схема работы блочного алгоритма в режиме обратной связи по выходу

При этом для каждого сеанса шифрования данных необходимо использовать новое начальное состояние регистра, которое может пересылаться по каналу открытым текстом.

Положим, $M = M_1 M_2...M_n$.

Для всех $i = 1...n$

$$C_i = M_i \oplus P_i,$$

где P_i — старшие k битов операции $E(C_{i-1})$.

Отличие от режима обратной связи по шифртексту состоит в методе обновления сдвигового регистра. Это осуществляется путем отбрасывания старших k битов и дописывания справа P_i.

Каждому из рассмотренных режимов (ECB, CBC, CFB, OFB) свойственны свои достоинства и недостатки, что обусловливает области их применения.

Режим ECB хорошо подходит для шифрования ключей; режим CFB, как правило, предназначается для шифрования отдельных символов, а режим OFB нередко применяется для шифрования в спутниковых системах связи.

Режимы CBC и CFB пригодны для аутентификации данных. Эти режимы позволяют также использовать блочные симметричные криптоалгоритмы для:

- интерактивного шифрования при обмене данными между терминалом и главной ЭВМ;
- шифрования криптографического ключа в практике автоматизированного распространения ключей;
- шифрования файлов, почтовых отправлений, данных спутников и других практических задач.

4.2.5. Особенности применения алгоритмов симметричного шифрования

Алгоритмы симметричного шифрования используют ключи относительно небольшой длины и могут быстро шифровать большие объемы данных. При симметричной методологии шифрования отправитель и получатель применяют для осуществления процессов шифрования и расшифрования сообщения один и тот же секретный ключ. Алгоритмы симметричного шифрования строятся исходя из предположения, что зашифрованные данные не сможет прочитать никто из тех, кто не обладает ключом для их расшифрования. Если ключ не был скомпрометирован, то при расшифровании автоматически выполняется аутентификация отправителя, так как только отправитель имеет ключ, с помощью которого можно зашифровать информацию, и только получатель имеет ключ, позволяющий расшифровать информацию.

Алгоритмы симметричного шифрования применяются для абонентского шифрования данных — т. е. для шифрования информации, предназначенной для отправки кому-либо, например, через Интернет. Использование только одного секретного ключа для всех абонентов сети, конечно, недопустимо по соображениям безопасности: в случае компрометации (утери, хищения) ключа под угрозой будет находиться документооборот всех абонентов сети.

Порядок использования систем с симметричными ключами:

1. Симметричный секретный ключ должен создаваться, распространяться и сохраняться безопасным образом.

2. Для получения зашифрованного текста отправитель применяет к исходному сообщению симметричный алгоритм шифрования вместе с секретным симметричным ключом. Таким образом неявно подготавливается аутентификация отправителя и получателя, так как только от-

правитель знает симметричный секретный ключ и может зашифровать этот текст. Только получатель знает симметричный секретный ключ и может расшифровать этот текст.

3. Отправитель передает зашифрованный текст. Симметричный секретный ключ никогда не передается в открытой форме по незащищенным каналам связи.

4. Получатель применяет к зашифрованному тексту тот же самый симметричный алгоритм шифрования/расшифрования вместе с тем же самым симметричным ключом (который уже есть у получателя) для восстановления исходного текста. Его успешное восстановление аутентифицирует того, кто знает секретный ключ.

Для симметричных криптосистем актуальна проблема безопасного распределения симметричных секретных ключей. Всем системам симметричного шифрования присущи следующие недостатки:

- принципиальным является требование защищенности и надежности канала передачи секретного ключа для каждой пары участников информационного обмена;
- предъявляются повышенные требования к службе генерации и распределения ключей, обусловленные тем, что для n абонентов при схеме взаимодействия «каждый с каждым» требуется $n(n-1)/2$ ключей; т. е. зависимость числа ключей от числа абонентов является квадратичной; например, для $n = 1000$ абонентов требуемое количество ключей будет равно $n(n-1)/2 = 499\,500$ ключей.

Поэтому без эффективной организации защищенного распределения ключей широкое использование обычной системы симметричного шифрования в больших сетях, и в частности в глобальных сетях, практически невозможно.

4.3. Асимметричные криптосистемы шифрования

Асимметричные криптографические системы были разработаны в 1970-х годах. Принципиальное отличие асимметричной криптосистемы от криптосистемы симметричного шифрования состоит в том, что для шифрования информации и ее последующего расшифрования используются различные ключи:

- *открытый ключ K:* используется для шифрования информации, вычисляется из секретного ключа k;
- *секретный ключ k:* используется для расшифрования информации, зашифрованной с помощью парного ему открытого ключа K.

Эти ключи различаются таким образом, что с помощью вычислений нельзя вывести секретный ключ k из открытого ключа K. Поэтому открытый ключ K может свободно передаваться по каналам связи.

Асимметричные системы называют еще двухключевыми криптографическими системами или криптосистемами с открытым ключом.

Обобщенная схема асимметричной криптосистемы шифрования с открытым ключом показана на рис. 4.18.

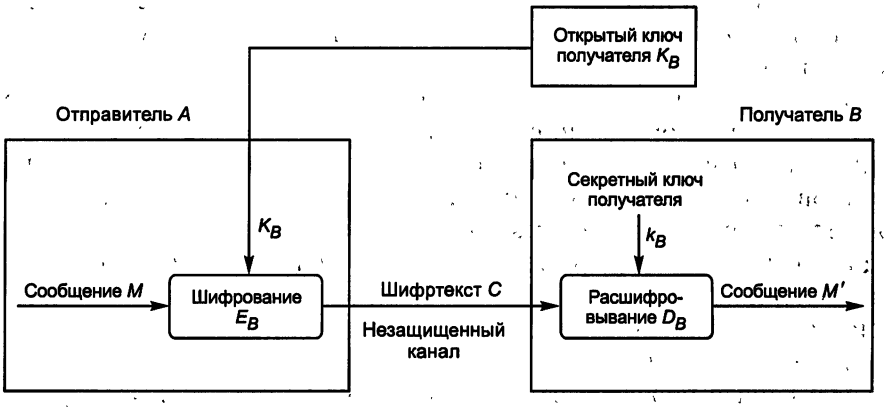


Рис. 4.18. Обобщенная схема асимметричной криптосистемы шифрования

Для криптографического закрытия и последующего расшифровывания передаваемой информации используются открытый и секретный ключи получателя *B* сообщения. В качестве ключа зашифровывания должен использоваться открытый ключ получателя, а в качестве ключа расшифровывания — его секретный ключ.

Секретный и открытый ключи генерируются попарно. Секретный ключ должен оставаться у его владельца, он должен быть надежно защищен от несанкционированного доступа (аналогично ключу шифрования в симметричных алгоритмах). Копия открытого ключа должна находиться у каждого абонента криптографической сети, с которым обменивается информацией владелец секретного ключа.

Процесс передачи зашифрованной информации в асимметричной криптосистеме осуществляется следующим образом:

1. Подготовительный этап:
- абонент *B* генерирует пару ключей: секретный ключ k_B и открытый ключ K_B;
- открытый ключ K_B посылается абоненту *A* и остальным абонентам (или делается доступным, например, на разделяемом ресурсе).

2. *Использование* — обмен информацией между абонентами *A* и *B*:
- абонент *A* зашифровывает сообщение с помощью открытого ключа K_B абонента *B* и отправляет шифртекст абоненту *B*;
- абонент *B* расшифровывает сообщение с помощью своего секретного ключа k_B. Никто другой (в том числе абонент *A*) не может расшифровать данное сообщение, так как не имеет секретного ключа абонента *B*. Защита информации в асимметричной криптосистеме основана на секретности ключа k_B получателя сообщения.

Отметим характерные особенности асимметричных криптосистем:

1. Открытый ключ K_B и криптограмма *C* могут быть отправлены по незащищенным каналам, т. е. противнику известны K_B и *C*.

2. Алгоритмы шифрования и расшифрования

$$E_B : M \to C;$$

$$D_B : C \to M$$

являются открытыми.

У. Диффи и М. Хеллман сформулировали требования, выполнение которых обеспечивает безопасность асимметричной криптосистемы [21]:

1. Вычисление пары ключей (K_B, k_B) получателем B на основе начального условия должно быть простым.

2. Отправитель A, зная открытый ключ K_B и сообщение M, может легко вычислить криптограмму

$$C = E_{K_B}(M).$$

3. Получатель B, используя секретный ключ k_B и криптограмму C, может легко восстановить исходное сообщение

$$M = D_{k_B}(C).$$

4. Противник, зная открытый ключ K_B, при попытке вычислить секретный ключ k_B наталкивается на непреодолимую вычислительную проблему.

5. Противник, зная пару (K_B, C), при попытке вычислить исходное сообщение M наталкивается на непреодолимую вычислительную проблему.

Концепция асимметричных криптографических систем с открытым ключом основана на применении однонаправленных функций.

Неформально *однонаправленную функцию* можно определить следующим образом [58]. Пусть X и Y — некоторые произвольные множества. Функция $f: X \to Y$ является однонаправленной, если для всех $x \in X$ можно легко вычислить функцию $y = f(x)$, где $y \in Y$.

И в то же время для большинства $y \in Y$ достаточно сложно получить значение $x \in X$, такое, что $f(x) = y$ (при этом полагают, что существует по крайней мере одно такое значение x).

Основным критерием отнесения функции f к классу однонаправленных функций является отсутствие эффективных алгоритмов обратного преобразования $Y \to X$.

В качестве примера однонаправленной функции можно указать *целочисленное умножение*. Прямая задача — вычисление произведения двух очень больших целых чисел P и Q, т. е. нахождение значения $N = P \times Q$ является относительно несложной задачей для компьютера.

Обратная задача — факторизация, или разложение на множители большого целого числа, т. е. нахождение делителей P и Q большого целого числа $N = P \times Q$, — является практически неразрешимой при достаточно больших значениях N. По современным оценкам теории чисел, при целом $N \approx 2^{664}$ и $P \approx Q$ для разложения числа N потребуется

около 10^{23} операций, т. е. задача практически неразрешима для современных компьютеров.

Другой характерный пример однонаправленной функции — это *модульная экспонента с фиксированными основанием и модулем.* Пусть A и N — целые числа, такие, что $1 \le A < N$. Определим множество Z_N:

$$Z_N = \{0, 1, 2, ..., N-1\}.$$

Тогда модульная экспонента с основанием A по модулю N представляет собой функцию

$$f_{A,N}: Z_N \to Z_N,$$

$$f_{A,N}(x) = A^x (\text{mod } N),$$

где X — целое число, $1 \le x \le N-1$.

Существуют эффективные алгоритмы, позволяющие достаточно быстро вычислить значения функции $f_{A,N}(x)$.

Если $y = A^x$, то естественно записать $x = \log_A(y)$.

Поэтому задачу обращения функции $f_{A,N}(x)$ называют задачей нахождения дискретного логарифма или задачей дискретного логарифмирования.

Задача дискретного логарифмирования формулируется следующим образом. Для известных целых A, N, y найти целое число x, такое, что

$$A^x \bmod N = y.$$

Алгоритм вычисления дискретного логарифма за приемлемое время пока не найден, поэтому модульная экспонента считается однонаправленной функцией.

По современным оценкам теории чисел, при целых числах $A \approx 2^{664}$ и $N \approx 2^{664}$ решение задачи дискретного логарифмирования (нахождение показателя степени x для известного y) потребует около 10^{26} операций, т. е. эта задача имеет в 10^3 раз большую вычислительную сложность, чем задача разложения на множители. При увеличении длины чисел разница в оценках сложности задач возрастает.

Следует отметить, что пока не удалось доказать невозможность существования эффективного алгоритма вычисления дискретного логарифма за приемлемое время. Исходя из этого модульная экспонента отнесена к однонаправленным функциям условно, что, однако, не мешает с успехом применять ее на практике.

Вторым важным классом функций, используемых при построении криптосистем с открытым ключом, являются так называемые *однонаправленные функции с секретом.* Дадим неформальное определение такой функции. Функция $f: X \to Y$ относится к классу однонаправленных функций с секретом в том случае, если она является однонаправленной и, кроме того, возможно эффективное вычисление обратной функции, если известен *секрет* (секретное число, строка или другая информация, ассоциирующаяся с данной функцией).

В качестве примера однонаправленной функции с секретом можно указать используемую в криптосистеме RSA модульную экспоненту с фиксированными модулем и показателем степени. Переменное основание модульной экспоненты используется для представления числового значения сообщения M либо криптограммы C.

Как и в случае симметричных криптографических систем, с помощью асимметричных криптосистем обеспечивается не только конфиденциальность, но также подлинность и целостность передаваемой информации. Подлинность и целостность любого сообщения обеспечивается формированием цифровой подписи этого сообщения и отправкой в зашифрованном виде сообщения вместе с цифровой подписью. Проверка соответствия подписи полученному сообщению после его предварительного расшифровывания представляет собой проверку целостности и подлинности принятого сообщения. Процедуры формирования и проверки электронной цифровой подписи рассмотрены в разделе 4.5.

Асимметричные криптографические системы обладают следующими важными преимуществами перед симметричными криптосистемами:

- в асимметричных криптосистемах решена сложная проблема распределения ключей между пользователями, так как каждый пользователь может сгенерировать свою пару ключей сам, а открытые ключи пользователей могут свободно публиковаться и распространяться по сетевым коммуникациям;
- исчезает квадратическая зависимость числа ключей от числа пользователей; в асимметричной криптосистеме количество используемых ключей связано с количеством абонентов линейной зависимостью (в системе из N пользователей используются $2 \times N$ ключей), а не квадратичной, как в симметричных системах;
- асимметричные криптосистемы позволяют реализовать протоколы взаимодействия сторон, которые не доверяют друг другу, поскольку при использовании асимметричных криптосистем закрытый ключ должен быть известен только его владельцу.

Однако у асимметричных криптосистем существуют и недостатки:

- на настоящий момент нет математического доказательства необратимости используемых в асимметричных алгоритмах функций;
- по сравнению с симметричным шифрованием асимметричное существенно медленнее, поскольку при шифровании и расшифровании используются весьма ресурсоемкие операции. По этой же причине реализовать аппаратный шифратор с асимметричным алгоритмом существенно сложнее, чем реализовать аппаратно симметричный алгоритм;
- необходимо защищать открытые ключи от подмены.

Последнее рассмотрим более подробно. Предположим, на компьютере абонента A хранится открытый ключ K_B абонента B. Злоумышленник n имеет доступ к открытым ключам, хранящимся у абонента A. Он генерирует свою пару ключей K_n и k_n и подменяет у абонента A открытый ключ K_B абонента B на свой открытый ключ K_n. Для того чтобы отправить некую информацию абоненту B, абонент A зашифровывает ее

на ключе K_n, думая, что это ключ K_B. Соответственно, это сообщение не сможет прочитать абонент B, но зато легко расшифрует и прочитает абонент n. От подмены открытых ключей может спасти процедура сертификации открытых ключей, которая рассмотрена в разделе 4.7.

4.3.1. Алгоритм шифрования RSA

Криптоалгоритм RSA предложили в 1978 г. три автора: Р. Райвест (Rivest), А. Шамир (Shamir) и Л. Эйдельман (Adleman). Алгоритм получил свое название по первым буквам фамилий его авторов. Алгоритм RSA стал первым алгоритмом с открытым ключом, который может работать как в режиме шифрования данных, так и в режиме электронной цифровой подписи.

Надежность алгоритма RSA основывается на трудности факторизации больших чисел и вычисления дискретных логарифмов в конечном поле.

В алгоритме RSA открытый ключ K_B, секретный ключ k_B, сообщение M и криптограмма C принадлежат множеству целых чисел

$$Z_N = \{0, 1, 2, \ldots, N-1\},$$

где N — модуль: $N = P \times Q$.

Здесь P и Q — случайные большие простые числа. Для обеспечения максимальной безопасности выбирают P и Q равной длины и хранят в секрете.

Множество Z_N с операциями сложения и умножения по модулю N образует арифметику по модулю N.

Открытый ключ K_B выбирают случайным образом так, чтобы выполнялись условия:

$$1 < K_B \le \varphi(N), \text{ НОД } (K_B, \varphi(N)) = 1;$$

$$\varphi(N) = (P-1)(Q-1),$$

где $\varphi(N)$ — функция Эйлера.

Функция Эйлера $\varphi(N)$ указывает количество положительных целых чисел в интервале от 1 до N, которые взаимно просты с N.

Второе из указанных выше условий означает, что открытый ключ K_B и функция Эйлера $\varphi(N)$ должны быть взаимно простыми.

Далее, используя расширенный алгоритм Евклида, вычисляют секретный ключ k_B, такой, что

$$k_B \times K_B \equiv 1 (\text{mod}\, \varphi(N))$$

или

$$k_B = K_B^{-1} (\text{mod}\, (P-1)(Q-1)).$$

Это можно осуществить, так как получатель B знает пару простых чисел (P, Q) и может легко найти $\varphi(N)$. Заметим, что k_B и N должны быть взаимно простыми.

Открытый ключ K_B используют для шифрования данных, а секретный ключ k_B — для расшифрования.

Процедура шифрования определяет криптограмму C через пару (открытый ключ K_B, сообщение M) в соответствии со следующей формулой:

$$C = E_{K_B}(M) = M^{K_B} (\mathrm{mod}\ N).$$

В качестве алгоритма быстрого вычисления значения C используют ряд последовательных возведений в квадрат целого M и умножений на M с приведением по модулю N.

Расшифрование криптограммы C выполняют, используя пару (секретный ключ k_B, криптограмма C) по следующей формуле:

$$M = D_{k_B}(C) = C^{k_B} (\mathrm{mod}\ N).$$

Процедуры шифрования и расшифрования в алгоритме RSA

Предположим, что пользователь A хочет передать пользователю B сообщение в зашифрованном виде, используя алгоритм RSA. В таком случае пользователь A выступает в роли отправителя сообщения, а пользователь B — в роли получателя. Как отмечалось выше, криптосистему RSA должен сформировать получатель сообщения, т. е. пользователь B. Рассмотрим последовательность действий пользователей B и A.

1. Пользователь B выбирает два произвольных больших простых числа P и Q.

2. Пользователь B вычисляет значение модуля $N = P \times Q$.

3. Пользователь B вычисляет функцию Эйлера

$$\varphi(N) = (P-1)(Q-1)$$

и выбирает случайным образом значение открытого ключа K_B с учетом выполнения условий

$$1 < K_B \le \varphi(N),\ \text{НОД}\ (K_B, \varphi(N)) = 1.$$

4. Пользователь B вычисляет значение секретного ключа k_B, используя расширенный алгоритм Евклида при решении сравнения

$$k_B \equiv K_B^{-1} (\mathrm{mod}\ \varphi(N)).$$

5. Пользователь B пересылает пользователю A пару чисел (N, K_B) по незащищенному каналу.

Если пользователь A хочет передать пользователю B сообщение M, он выполняет следующие шаги.

6. Пользователь A разбивает исходный открытый текст M на блоки, каждый из которых может быть представлен в виде числа

$$M_i = 0, 1, 2, \ldots, N-1.$$

7. Пользователь A шифрует текст, представленный в виде последовательности чисел M_i по формуле

$$C_i = M_i^{K_B} (\mathrm{mod}\, N)$$

и отправляет криптограмму

$$C_1,\ C_2,\ C_3,\ ...,\ C_i,\ ...$$

пользователю B.

8. Пользователь B расшифровывает принятую криптограмму

$$C_1,\ C_2,\ C_3,\ ...,\ C_i,\ ...,$$

используя секретный ключ k_B, по формуле

$$M_i = C_i^{k_B} (\mathrm{mod}\, N).$$

В результате будет получена последовательность чисел M_i, которые представляют собой исходное сообщение M. При практической реализации алгоритма RSA необходимо иметь возможность без существенных затрат генерировать большие простые числа, уметь оперативно вычислять значения ключей K_B и k_B.

Пример. Шифрование сообщения С А В. Для простоты вычислений будут использоваться небольшие числа. На практике применяются очень большие числа (длиной 250—300 десятичных разрядов).

Действия пользователя В.

1. Выбирает $P = 3$ и $Q = 11$.
2. Вычисляет модуль $N = P \times Q = 3 \times 11 = 33$.
3. Вычисляет значение функции Эйлера для $N = 33$:

$$\varphi(N) = \varphi(33) = (P - 1)(Q - 1) = 2 \times 10 = 20.$$

Выбирает в качестве открытого ключа K_B произвольное число с учетом выполнения условий

$$1 < K_B \le 20,\ \text{НОД}\ (K_B,\ 20) = 1.$$

Пусть $K_B = 7$.

4. Вычисляет значение секретного ключа k_B, используя расширенный алгоритм Евклида при решении сравнения

$$k_B \equiv 7^{-1} (\mathrm{mod}\, 20).$$

Решение дает $k_B = 3$.

5. Пересылает пользователю A пару чисел ($N = 33$, $K_B = 7$).

Действия пользователя А.

6. Представляет шифруемое сообщение как последовательность целых чисел в диапазоне 0...32. Пусть буква А представляется как число 1, буква В — как число 2, буква С — как число 3. Тогда сообщение С А В

можно представить как последовательность чисел 312, т. е. $M_1 = 3$, $M_2 = 1$, $M_3 = 2$.

7. Шифрует текст, представленный в виде последовательности чисел M_1, M_2 и M_3, используя ключ $K_B = 7$ и $N = 33$, по формуле

$$C_i = M_i^{K_B} (\text{mod } N) = M_i^7 (\text{mod } 33),$$

получает

$C_1 = 3^7 (\text{mod } 33) = 2187 (\text{mod } 33) = 9;$

$C_2 = 1^7 (\text{mod } 33) = 1 (\text{mod } 33) = 1;$

$C_3 = 2^7 (\text{mod } 33) = 128 (\text{mod } 33) = 29.$

Отправляет пользователю B криптограмму

$$C_1, C_2, C_3 = 9, 1, 29.$$

Действия пользователя B.

8. Расшифровывает принятую криптограмму C_1, C_2, C_3, используя секретный ключ $k_B = 3$, по формуле

$$M_i = C_i^{k_B} (\text{mod } N) = C_i^3 (\text{mod } 33).$$

Получает

$M_1 = 9^3 (\text{mod } 33) = 729 (\text{mod } 33) = 3;$

$M_2 = 1^3 (\text{mod } 33) = 1 (\text{mod } 33) = 1;$

$M_3 = 29^3 (\text{mod } 33) = 24\,389 (\text{mod } 33) = 2.$

Таким образом, восстановлено исходное сообщение:

C	A	B
3	1	2

Криптоалгоритм RSA всесторонне исследован и признан стойким при достаточной длине ключей. В настоящее время длина ключа 1024 бит считается приемлемым вариантом. Некоторые авторы утверждают, что с ростом мощности процессоров криптоалгоритм RSA потеряет стойкость к атаке полного перебора. Однако увеличение мощности процессоров позволит применить более длинные ключи, что повышает стойкость RSA. Следует отметить, что алгоритм RSA можно применять как для шифрования сообщений, так и для электронной цифровой подписи.

Нетрудно видеть, что в асимметричной криптосистеме RSA количество используемых ключей связано с количеством абонентов линейной зависимостью (в системе из N пользователей используются $2 \times N$ ключей), а не квадратичной, как в симметричных системах.

Сравнивая наиболее популярных представителей асимметричного и симметричного шифрования, следует отметить, что по быстродействию RSA существенно уступает DES, а программная и аппаратная реализация криптоалгоритма RSA гораздо сложнее, чем DES. Поэтому криптосистема RSA, как правило, используется при передаче небольшого объема сообщений.

4.3.2. Асимметричные криптосистемы на базе эллиптических кривых

К криптосистемам третьего тысячелетия, несомненно, следует отнести асимметричные криптосистемы на базе эллиптических кривых. Криптосистемы на базе эллиптических кривых позволяют реализовать криптоалгоритм асимметричного шифрования, протокол выработки разделяемого секретного ключа для симметричного шифрования и криптоалгоритмы электронной цифровой подписи [7, 38].

Криптосистемы на базе эллиптических кривых имеют более высокую производительность и позволяют использовать существенно меньшие размеры ключей при сохранении требуемого уровня безопасности.

Для различных реализаций используются эллиптические кривые двух видов:

- эллиптическая кривая в конечном поле F_p, где p — простое число, $p > 3$;
- эллиптическая кривая в конечном поле F_2^m.

Эллиптическая кривая в конечном поле F_p. Пусть задано простое число $p > 3$. Тогда *эллиптической кривой* E, определенной над конечным простым полем F_p, называется множество пар чисел (x, y), $x \in F_p$, $y \in F_p$, удовлетворяющих тождеству

$$y^2 \equiv x^3 + ax + b \pmod{p}, \qquad (*)$$

где $a, b \in F_p$ и $4a^3 + 27b^2$ не сравнимо с нулем по модулю p.

Инвариантом эллиптической кривой называется величина $J(E)$, удовлетворяющая тождеству

$$J(E) = 1728\frac{4a^3}{4a^3 + 27b^2} \pmod{P}.$$

Коэффициенты a, b эллиптической кривой E по известному инварианту $J(E)$ определяются следующим образом:

$$\begin{cases} a \equiv 3k \pmod{p}; \\ b \equiv 2k \pmod{p}, \end{cases}$$

где $k = \dfrac{J(E)}{1728 - J(E)} \pmod{p}$, $J(E) \neq 0$, или 1728.

Пары (x, y), удовлетворяющие тождеству (*), называются *точками эллиптической кривой* E; x и y — соответственно x- и y-координатами точки.

Точки эллиптической кривой будем обозначать $Q(x; y)$ или просто Q. Две точки эллиптической кривой равны, если равны их соответствующие x- и y-координаты.

На множестве всех точек эллиптической кривой E введем *операцию сложения*, которую будем обозначать знаком +. Для двух произвольных

точек $Q_1(x_1, y_1)$ и $Q_2(x_2, y_2)$ эллиптической кривой E рассмотрим несколько вариантов.

Пусть координаты точек Q_1 и Q_2 удовлетворяют условию $x_1 \neq x_2$. В этом случае их суммой будем называть точку $Q_3(x_3, y_3)$, координаты которой определяются сравнениями

$$\begin{cases} x_3 \equiv \lambda^2 - x_1 - x_2 (\mathrm{mod}\ p); \\ y_3 \equiv \lambda(x_1 - x_3) - y_1 (\mathrm{mod}\ p), \end{cases}$$

где $\lambda \equiv \dfrac{y_2 - y_1}{x_2 - x_1} (\mathrm{mod}\ p)$.

Если выполнены равенства $x_1 = x_2$ и $y_1 = y_2 \neq 0$, то определим координаты точки Q_3 следующим образом:

$$\begin{cases} x_3 \equiv \lambda^2 - 2x_1 (\mathrm{mod}\ p); \\ y_3 \equiv \lambda(x_1 - x_3) - y_1 (\mathrm{mod}\ p), \end{cases}$$

где $\lambda \equiv \dfrac{3x_1^2 + a}{2y_1} (\mathrm{mod}\ p)$.

В случае, когда выполнено условие $x_1 = x_2$ и $y_1 = -y_2 \pmod p$, сумму точек Q_1 и Q_2 будем называть *нулевой точкой* O, не определяя ее x- и y-координаты. В этом случае точка Q_2 называется *отрицанием* точки Q_1. Для нулевой точки O выполнены равенства

$$Q + O = O + Q = Q,$$

где Q — произвольная точка эллиптической кривой E.

Относительно введенной операции сложения множество всех точек эллиптической кривой E вместе с нулевой точкой образуют *конечную абелеву (коммутативную) группу порядка* m, для которого выполнено неравенство

$$p + 1 - 2\sqrt{p} \leq m \leq p + 1 + 2\sqrt{p}.$$

Точка Q называется точкой кратности k, или просто кратной точкой эллиптической кривой E, если для некоторой точки P выполнено равенство

$$Q = \underbrace{P + \ldots + P}_{k} = kP.$$

Эллиптическая кривая в конечном поле F_2^m определяется соотношением

$$y^2 + xy \equiv x^3 + ax^2 + b$$

при ненулевом b.

Эллиптической кривой $E(F_{2^m})$ является группа решений (x, y), $x \in F_{2^m}$, $y \in F_{2^m}$ приведенного выше соотношения при определенных значениях a и b, а также нулевая точка O.

Аналогично группе эллиптической кривой $E(F_p)$, множество всех точек эллиптической кривой $E(F_{2^m})$ вместе с нулевой точкой образуют конечную абелеву группу.

С помощью описанных выше правил сложения можно вычислить точку kP для любого целого числа k и любой точки P эллиптической кривой.

Однако решение обратной задачи — нахождение числа k по известным точкам P и kP — является трудноразрешимой проблемой. Данную задачу называют *проблемой дискретного логарифма эллиптической кривой ECDLP (Elliptic Curve Discrete Logariphm Problem)*. Решение проблемы ECDLP является значительно более сложным, чем проблемы дискретного логарифмирования (нахождение числа x по заданному числу $y = g^x \bmod p$ при известных основании g и модуле p), на которой базируются RSA-подобные асимметричные криптосистемы.

Сложность решения проблемы ECDLP обусловлена ресурсоемкостью операций сложения и дублирования точек, с помощью которых вычисляется kP, как видно из приведенных выше формул. Отсюда следует возможность применения более коротких ключей. Например, ключу размером 1024 бит алгоритма DSA соответствует по криптостойкости ключ размером 160 бит алгоритма ECDSA (DSA на эллиптических кривых).

Существует несколько реализаций известных криптоалгоритмов на базе эллиптических кривых (стандартизованы в IEEE P1363).

4.3.3. Алгоритм асимметричного шифрования ECES

В алгоритме ECES (Elliptic Curve Encryption Scheme) сначала должны быть определены следующие параметры, являющиеся открытой информацией, общей для всех пользователей системы [7, 38]:

- конечное поле F_q;
- эллиптическая кривая $E(F_q)$;
- большой простой делитель количества точек кривой n;
- точка P, координаты которой должны иметь тот же порядок, что и число n.

Каждый пользователь системы генерирует пару ключей следующим образом:

- выбирается случайное целое число d, $1 < d < n - 1$;
- вычисляется точка $Q = dP$.

Секретным ключом пользователя является число d, открытым ключом — точка Q.

Зашифрование сообщения (пользователь A шифрует сообщение M для пользователя B):

- сообщение разбивается на блоки M_i, которые определенным образом дополняются слева (длина каждого блока равна $2L - 16$ бит, где L равно ближайшему большему целому от $\log_2 q$);

- полученный блок разбивается на две части равной длины: m_{i1} и m_{i2};
- выбирается случайное целое число k, $1 < k < n - 1$;
- вычисляется точка $(x_1, y_1) = kP$;
- вычисляется точка $(x_2, y_2) = kQ_B$;
- с помощью определенного преобразования из m_{i1}, m_{i2} и x_2 получают c_1 и c_2;
- зашифрованные данные: (x_1, y_1, c_1, c_2).

Расшифрование сообщения (пользователь B расшифровывает полученное от пользователя A зашифрованное сообщение):

- вычисляется точка $(x_2, y_2) = d(x_1, y_1)$;
- восстанавливается исходное сообщение m_{i1}, m_{i2} из c_1, c_2 и x_2.

4.4. Функция хэширования

Функция хэширования (хэш-функция) представляет собой преобразование, на вход которого подается сообщение переменной длины M, а выходом является строка фиксированной длины $h(M)$. Иначе говоря, хэш-функция $h(\cdot)$ принимает в качестве аргумента сообщение (документ) M произвольной длины и возвращает хэш-значение (хэш) $H = h(M)$ фиксированной длины (рис. 4.19).

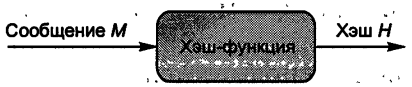


Рис. 4.19. Схема формирования хэша $H = h(M)$

Хэш-значение $h(M)$ — это *дайджест сообщения* M, т. е. сжатое двоичное представление основного сообщения M произвольной длины. Хэш-значение $h(M)$ формируется функцией хэширования.

Функция хэширования позволяет сжать подписываемый документ M до 128 и более битов (в частности, 128 или 256 бит), тогда как M может быть размером в мегабайт или более. Следует отметить, что значение хэш-функции $h(M)$ зависит сложным образом от документа M и не позволяет восстановить сам документ M.

Функция хэширования должна обладать следующими свойствами:

1. Хэш-функция может быть применена к аргументу любого размера.
2. Выходное значение хэш-функции имеет фиксированный размер.
3. Хэш-функцию $h(x)$ достаточно просто вычислить для любого x. Скорость вычисления хэш-функции должна быть такой, чтобы скорость выработки и проверки ЭЦП при использовании хэш-функции была значительно больше, чем при использовании самого сообщения.
4. Хэш-функция должна быть чувствительна ко всевозможным изменениям в тексте M, таким как вставки, выбросы, перестановки и т. п.
5. Хэш-функция должна быть однонаправленной, т. е. обладать свойством необратимости, иными словами, задача подбора докумен-

та M', который обладал бы требуемым значением хэш-функции, должна быть вычислительно неразрешима.

6. Вероятность того, что значения хэш-функций двух различных документов (вне зависимости от их длин) совпадут, должна быть ничтожно мала; т. е. для любого фиксированного x с вычислительной точки зрения невозможно найти $x' \neq x$, такое, что $h(x') = h(x)$.

Теоретически возможно, что два различных сообщения могут быть сжаты в одну и ту же свертку (так называемая коллизия, или столкновение). Поэтому для обеспечения стойкости функции хэширования необходимо предусмотреть способ избегать столкновений. Полностью столкновений избежать нельзя, поскольку в общем случае количество возможных сообщений превышает количество возможных выходных значений функции хэширования. Однако вероятность столкновения должна быть низкой.

Свойство 5 эквивалентно тому, что $h(\,)$ является односторонней функцией. Свойство 6 гарантирует, что не может быть найдено другое сообщение, дающее ту же свертку. Это предотвращает фальсификацию сообщения.

Таким образом, функция хэширования может использоваться для обнаружения изменений сообщения, т. е. она может служить для формирования *криптографической контрольной суммы* (также называемой кодом обнаружения изменений или *кодом аутентификации сообщения*). В этом качестве хэш-функция используется для контроля целостности сообщения, при формировании и проверке электронной цифровой подписи.

Хэш-функции широко используются также в целях аутентификации пользователей. В ряде технологий информационной безопасности применяется своеобразный прием шифрования — *шифрование с помощью односторонней хэш-функции*. Своеобразие этого шифрования заключается в том, что оно, по существу, является односторонним, т. е. не сопровождается обратной процедурой — расшифрованием на приемной стороне. Обе стороны (отправитель и получатель) используют одну и ту же процедуру одностороннего шифрования на основе хэш-функции [7, 63]. Применение в протоколах аутентификации односторонних функций шифрования на основе ключевых хэш-функций рассматривается в главе 5.

Известные функции хэширования:

- отечественный стандарт ГОСТ Р34.11—94 [11]. Вычисляет хэш размером 32 байта;
- MD (Message Digest) — ряд алгоритмов хэширования, наиболее распространенных в мире. Каждый из них вырабатывает 128-битный хэш-код. Алгоритм MD2 — самый медленный из них, MD4 — самый быстрый. Алгоритм MD5 является модификацией MD4, при которой пожертвовали скоростью ради увеличения безопасности. Алгоритм MD5 применяется в последних версиях Microsoft Windows для преобразования пароля пользователя в 16-байтное число [7, 63];

- SHA (Secure Hash Algorithm) — это алгоритм вычисления дайджеста сообщений, вырабатывающий 160-битный хэш-код входных данных; широко распространен в мире, используется во многих сетевых протоколах защиты информации.

Хэш-функции широко используются также для аутентификации пользователей. Существует множество криптографических протоколов, основанных на применении хэш-функций (см. главу 5).

Отечественный стандарт хэширования ГОСТ Р 34.11—94

Отечественным стандартом генерирования хэш-функции является алгоритм ГОСТ Р 34.11—94. Этот стандарт является обязательным для применения в качестве алгоритма хэширования в государственных организациях РФ и ряде коммерческих организаций. Коротко данный алгоритм хэширования можно описать следующим образом (рис. 4.20).

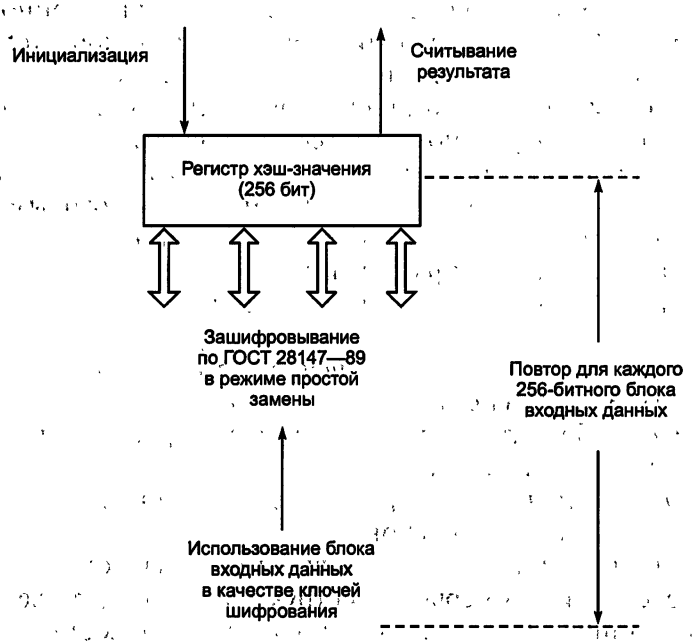


Рис. 4.20. Хэширование по алгоритму ГОСТ Р 34.11—94

Шаг 1. Инициализация регистра хэш-значения. Если длина сообщения не превышает 256 бит — переход к шагу 3, если превышает — переход к шагу 2.

Шаг 2. Итеративное вычисление хэш-значения блоков хэшируемых данных по 256 бит с использованием хранящегося в регистре хэш-значения предыдущего блока. Вычисление включает в себя следующие действия:

- генерацию ключей шифрования на основе блока хэшируемых данных;

- зашифрование хранящегося в регистре хэш-значения в виде четырех блоков по 64 бит по алгоритму ГОСТ 28147–89 в режиме простой замены;
- перемешивание результата.

Вычисление производится до тех пор, пока длина необработанных входных данных не станет меньше или равной 256 бит. В этом случае — переход к шагу 3.

Шаг 3. Дополнение битными нулями необработанной части сообщения до 256 бит. Вычисление хэш-значения аналогично шагу 2. В результате в регистре оказывается искомое хэш-значение.

4.5. Электронная цифровая подпись

Электронная цифровая подпись (ЭЦП) используется для аутентификации текстов, передаваемых по телекоммуникационным каналам. При таком обмене электронными документами существенно снижаются затраты на обработку и хранение документов, ускоряется их поиск. Но возникает проблема аутентификации автора электронного документа и самого документа, т. е. установления подлинности автора и отсутствия изменений в полученном электронном документе.

Целью аутентификации электронных документов является их защита от возможных видов злоумышленных действий, к которым относятся:

- *активный перехват* — нарушитель, подключившийся к сети, перехватывает документы (файлы) и изменяет их;
- *маскарад* — абонент *C* посылает документ абоненту *B* от имени абонента *A*;
- *ренегатство* — абонент *A* заявляет, что не посылал сообщения абоненту *B*, хотя на самом деле послал;
- *подмена* — абонент *B* изменяет или формирует новый документ и заявляет, что получил его от абонента *A*;
- *повтор* — абонент *C* повторяет ранее переданный документ, который абонент *A* посылал абоненту *B*.

Эти виды злоумышленных действий могут нанести существенный ущерб банковским и коммерческим структурам, государственным предприятиям и организациям, частным лицам, применяющим в своей деятельности компьютерные информационные технологии.

Проблему проверки целостности сообщения и подлинности автора сообщения позволяет эффективно решить методология электронной цифровой подписи.

4.5.1. Основные процедуры цифровой подписи

Функционально цифровая подпись аналогична обычной рукописной подписи и обладает ее основными достоинствами:

- удостоверяет, что подписанный текст исходит от лица, поставившего подпись;

- не дает самому этому лицу возможности отказаться от обязательств, связанных с подписанным текстом;
- гарантирует целостность подписанного текста.

Электронная цифровая подпись представляет собой относительно небольшое количество дополнительной цифровой информации, передаваемой вместе с подписываемым текстом.

ЭЦП основана на обратимости асимметричных шифров, а также на взаимосвязанности содержимого сообщения, самой подписи и пары ключей. Изменение хотя бы одного из этих элементов сделает невозможным подтверждение подлинности цифровой подписи. ЭЦП реализуется при помощи асимметричных алгоритмов шифрования и хэш-функций.

Технология применения системы ЭЦП предполагает наличие сети абонентов, посылающих друг другу подписанные электронные документы. Для каждого абонента генерируется пара ключей: секретный и открытый. Секретный ключ хранится абонентом в тайне и используется им для формирования ЭЦП. Открытый ключ известен всем другим пользователям и предназначен для проверки ЭЦП получателем подписанного электронного документа.

Система ЭЦП включает две основные процедуры:

- формирования цифровой подписи;
- проверки цифровой подписи.

В процедуре формирования подписи используется секретный ключ отправителя сообщения, в процедуре проверки — открытый ключ отправителя.

Процедура формирования цифровой подписи

На подготовительном этапе этой процедуры абонент A — отправитель сообщения — генерирует пару ключей: секретный ключ k_A и открытый ключ K_A. Открытый ключ K_A вычисляется из парного ему секретного ключа k_A. Открытый ключ K_A рассылается остальным абонентам сети (или делается доступным, например, на разделяемом ресурсе) для использования при проверке подписи. Для формирования цифровой подписи отправитель A прежде всего вычисляет значение хэш-функции $h(M)$ подписываемого текста M (рис. 4.21).

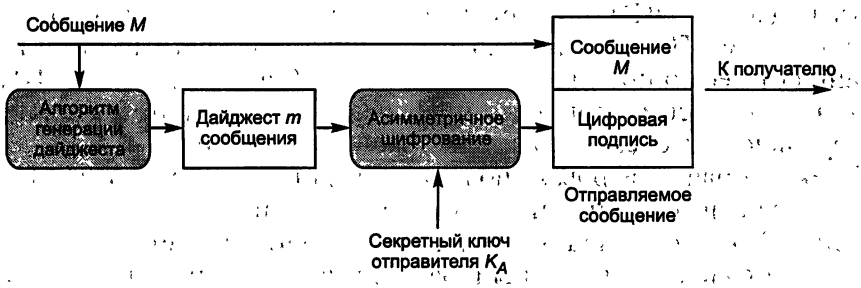


Рис. 4.21. Схема формирования электронной цифровой подписи

Хэш-функция служит для сжатия исходного подписываемого текста M в дайджест — относительно короткое число, состоящее из фиксированного небольшого числа битов и характеризующее весь текст M в целом (см. раздел 4.4). Далее отправитель A шифрует дайджест m своим секретным ключом k_A. Получаемая при этом пара чисел представляет собой цифровую подпись для данного текста M. Сообщение M вместе с цифровой подписью отправляется в адрес получателя.

Процедура проверки цифровой подписи

Абоненты сети могут проверить цифровую подпись полученного сообщения M с помощью открытого ключа отправителя K_A этого сообщения (рис. 4.22).

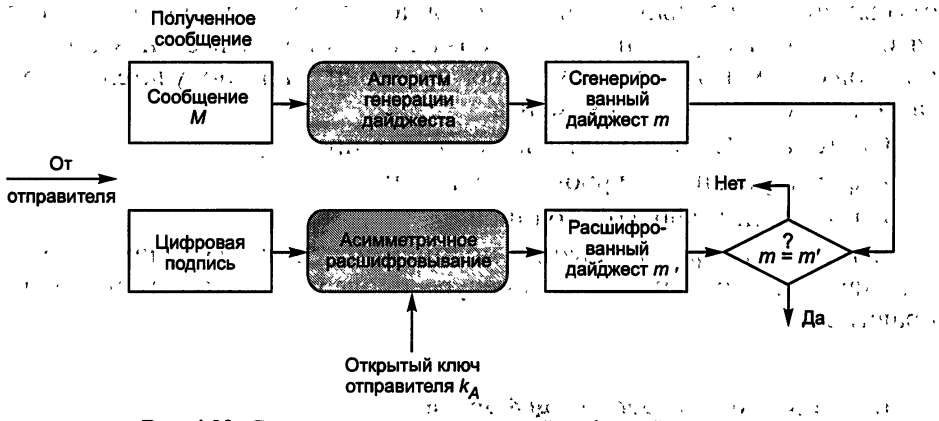


Рис. 4.22. Схема проверки электронной цифровой подписи

При проверке ЭЦП абонент B — получатель сообщения M — расшифровывает принятый дайджест m открытым ключом K_A отправителя A. Кроме того, получатель сам вычисляет с помощью хэш-функции $h(M)$ дайджест m' принятого сообщения M и сравнивает его с расшифрованным. Если эти два дайджеста m и m' совпадают, то цифровая подпись является подлинной. В противном случае либо подпись подделана, либо изменено содержание сообщения.

Принципиальным моментом в системе ЭЦП является невозможность подделки ЭЦП пользователя без знания его секретного ключа подписывания. Поэтому необходимо защитить секретный ключ подписывания от несанкционированного доступа. Секретный ключ ЭЦП аналогично ключу симметричного шифрования рекомендуется хранить на персональном ключевом носителе в защищенном виде.

Электронная цифровая подпись представляет собой уникальное число, зависящее от подписываемого документа и секретного ключа абонента. В качестве подписываемого документа может быть использован любой файл. Подписанный файл создается из неподписанного путем добавления в него одной или более электронных подписей.

Помещаемая в подписываемый файл (или в отдельный файл электронной подписи) структура ЭЦП обычно содержит дополнительную информацию, однозначно идентифицирующую автора подписанного документа. Эта информация добавляется к документу до вычисления ЭЦП, что обеспечивает и ее целостность. Каждая подпись содержит следующую информацию:

- дату подписи;
- срок окончания действия ключа данной подписи;
- информацию о лице, подписавшем файл (Ф.И.О., должность, краткое наименование фирмы);
- идентификатор подписавшего (имя открытого ключа);
- собственно цифровую подпись.

Важно отметить, что, с точки зрения конечного пользователя, процесс формирования и проверки цифровой подписи отличается от процесса криптографического закрытия передаваемых данных следующими особенностями.

При формировании цифровой подписи используется закрытый ключ отправителя, тогда как при зашифровывании применяется открытый ключ получателя. При проверке цифровой подписи используется открытый ключ отправителя, а при расшифровывании — закрытый ключ получателя.

Проверить сформированную подпись может любое лицо, так как ключ проверки подписи является открытым. При положительном результате проверки подписи делается заключение о подлинности и целостности полученного сообщения, т. е. о том, что это сообщение действительно отправлено тем или иным отправителем и не было модифицировано при передаче по сети. Однако, если пользователя интересует, не является ли полученное сообщение повторением ранее отправленного или не было ли оно задержано на пути следования, то он должен проверить дату и время его отправки, а при наличии — порядковый номер.

Аналогично асимметричному шифрованию, необходимо обеспечить невозможность подмены открытого ключа, используемого для проверки ЭЦП. Если предположить, что злоумышленник n имеет доступ к открытым ключам, которые хранит на своем компьютере абонент B, в том числе к открытому ключу K_A абонента A, то он может выполнить следующие действия:

- прочитать из файла, в котором содержится открытый ключ K_A, идентификационную информацию об абоненте A;
- сгенерировать собственную пару ключей k_n и K_n, записав в них идентификационную информацию абонента A;
- подменить хранящийся у абонента B открытый ключ K_A своим открытым ключом K_n, но содержащим идентификационную информацию абонента A.

После этого злоумышленник n может посылать документы абоненту B, подписанные своим секретным ключом k_n. При проверке подписи этих документов абонент B будет считать, что документы подписаны абонентом A и их ЭЦП верна, т. е. они не были модифицированы

кем-либо. До выяснения отношений непосредственно с абонентом A у абонента B может не появиться сомнений в подлинности полученных документов. Открытые ключи ЭЦП можно защитить от подмены с помощью соответствующих цифровых сертификатов (см. раздел 4.7).

Сегодня существует большое количество алгоритмов ЭЦП.

4.5.2. Алгоритм цифровой подписи DSA

Алгоритм цифровой подписи DSA (Digital Signature Algorithm) был предложен в 1991 г. Национальным институтом стандартов и технологий США (National Institute of Standards and Technology — NIST) и стал стандартом США в 1993 г. Алгоритм DSA является развитием алгоритмов цифровой подписи Эль Гамаля и К. Шнорра [7, 63]. Ниже приводятся процедуры генерации ключей, генерации подписи и проверки подписи в алгоритме DSA.

Генерация ключей DSA. Отправитель и получатель электронного документа используют при вычислениях большие целые числа: g и p — простые числа, длиной L битов каждое ($512 \le L \le 1024$); q — простое число длиной 160 бит (делитель числа $(p-1)$). Числа g, p, q являются открытыми и могут быть общими для всех пользователей сети.

Отправитель выбирает случайное целое число x, $1 < x < q$. Число x является *секретным ключом отправителя* для формирования электронной цифровой подписи.

Затем отправитель вычисляет значение

$$y = g^x \bmod p.$$

Число y является *открытым ключом* для проверки подписи отправителя. Число y передается всем получателям документов.

Генерация подписи DSA. Этот алгоритм предусматривает использование односторонней функции хэширования $h(\cdot)$. В стандарте определен алгоритм безопасного хэширования SHA-1.

Для того чтобы подписать сообщение M, участник A выполняет следующие шаги:

1. Выбирает случайное целое k в интервале $[1, q-1]$.
2. Вычисляет $r = (g^k \bmod p) \bmod q$.
3. Вычисляет $k^{-1} \bmod q$.
4. Вычисляет $s = k^{-1}\{h(M) + xr\} \bmod q$, где h есть алгоритм хэширования SHA-1.
5. Если $s = 0$, тогда перейти к шагу 1. (Если $s = 0$, тогда $s^{-1} \bmod q$ не существует; s требуется на шаге 2 процедуры проверки подписи.)
6. Подпись для сообщения M есть пара целых чисел (r, s).

Проверка подписи DSA. Для того чтобы проверить подпись (r, s) на M участника A, участник B делает следующие шаги:

1. Получает подлинную копию открытого ключа y участника A.
2. Вычисляет $w = s^{-1} \bmod q$ и хэш-значение $h(M)$.
3. Вычисляет значения $u_1 = h(M)w \bmod q$ и $u_2 = (rw) \bmod q$.

4. Используя открытый ключ y, вычисляет значение $v = (g^{u1} y^{u2} \bmod p) \bmod q$.

5. Признает подпись (r, s) под документом M подлинной, если $v = r$.

Поскольку r и s являются целыми числами, причем каждое меньше q, подписи DSA имеют длину 320 бит. Безопасность алгоритма цифровой подписи DSA базируется на трудностях задачи дискретного логарифмирования.

4.5.3. Алгоритм цифровой подписи ECDSA

В алгоритме ЭЦП ECDSA (Elliptic Curve Digital Signature Algorithm) определение параметров системы и генерация ключей аналогичны алгоритму асимметричного шифрования ECES.

Генерация ЭЦП (пользователь A подписывает сообщение M):

- вычисляется хэш собщения $H(M)$;
- выбирается случайное целое число k, взаимно простое с n (т. е. не имеющее других общих с n делителей, кроме 1; поскольку n является простым числом по определению, данное условие выполняется автоматически), $1 < k < n - 1$;
- вычисляется точка $(x_1, y_1) = kP$ и $r = x_1 \bmod n$. В случае если $r = 0$, повторяется выбор k;
- вычисляется $s = k^{-1}(H(M) + rd) \bmod n$;
- цифровой подписью сообщения M является пара чисел (r, s).

Проверка ЭЦП (пользователь B проверяет ЭЦП пользователя A под сообщением M):

- если $r = 0$, то полученная ЭЦП неверна;
- вычисляется хэш сообщения $H(M)$;
- вычисляются $u = s^{-1}H(M) \bmod n$ и $v = s^{-1}r \bmod n$;
- вычисляется точка $(x_1, y_1) = uP + vQ$;
- вычисляется $r' = x_1 \bmod n$;
- ЭЦП считается верной, если $r' = r$.

4.5.4. Алгоритм цифровой подписи ГОСТ Р 34.10—94

Первый отечественный стандарт цифровой подписи обозначается как ГОСТ Р 34.10—94 [10]. Алгоритм цифровой подписи, определяемый этим стандартом, концептуально близок к алгоритму DSA. В нем используются следующие параметры:

- p — большое простое число длиной от 509 до 512 бит либо от 1020 до 1024 бит;
- q — простой сомножитель числа $(p - 1)$, имеющий длину 254—256 бит;
- a — любое число, меньшее $(p - 1)$, причем такое, что $a^q \bmod p = 1$;
- x — некоторое число, меньшее q;
- $y = a^x \bmod p$.

Кроме того, этот алгоритм использует однонаправленную хэш-функцию $H(x)$. Стандарт ГОСТ Р 34.11—94 определяет хэш-функцию, основанную на использовании стандартного симметричного алгоритма ГОСТ 28147—89.

Первые три параметра p, q и a являются открытыми и могут быть общими для всех пользователей сети. Число x является секретным ключом. Число y является открытым ключом.

Чтобы подписать некоторое сообщение m, а затем проверить подпись, выполняются следующие шаги.

1. Пользователь A генерирует случайное число k, причем $k < q$.

2. Пользователь A вычисляет значения

$$r = (a^k \bmod p) \bmod q,$$

$$s = (x \times r + k(H(m))) \bmod q.$$

Если $H(m) \bmod q = 0$, то значение $H(m) \bmod q$ принимают равным единице. Если $r = 0$, то выбирают другое значение k и начинают снова. Цифровая подпись представляет собой два числа: $r \bmod 2^{256}$ и $s \bmod 2^{256}$.

Пользователь A отправляет эти числа пользователю B.

3. Пользователь B проверяет полученную подпись, вычисляя

$$v = H(m)^{q-2} \bmod q,$$

$$z_1 = (s * v) \bmod q,$$

$$z_2 = ((q - r) * v) \bmod q,$$

$$u = (a^{z_1} \times y^{z_2}) \bmod p) \bmod q.$$

Если $u = r$, то подпись считается верной.

Различие между этим алгоритмом и алгоритмом DSA заключается в том, что в DSA

$$s = (k^{-1}(x \times r + (H(m)))) \bmod q,$$

что приводит к другому уравнению верификации.

Следует также отметить, что в отечественном стандарте ЭЦП параметр q имеет длину 256 бит. Западных криптографов вполне устраивает q длиной примерно 160 бит. Различие в значениях параметра q является отражением стремления разработчиков отечественного стандарта к получению более безопасной подписи. Этот стандарт вступил в действие с начала 1995 г.

4.5.5. Отечественный стандарт цифровой подписи ГОСТ Р 34.10—2001

Отечественный стандарт цифровой подписи ГОСТ Р 34.10—2001 был принят в 2001 г. [9]. Этот стандарт разработан взамен первого стандарта цифровой подписи ГОСТ Р 34.10—94. Необходимость разработки

стандарта ГОСТ Р 34.10—2001 вызвана потребностью в повышении стойкости электронной цифровой подписи к несанкционированным изменениям. Стойкость ЭЦП основывается на сложности вычисления дискретного логарифма в группе точек эллиптической кривой, а также на стойкости используемой хэш-функции по ГОСТ Р 34.11.

Принципиальное отличие нового стандарта от предыдущего ГОСТ Р 34.10—94 состоит в том, что все вычисления при генерации и проверке ЭЦП в новом алгоритме производятся в группе точек эллиптической кривой, определенной над конечным полем F_p.

Принадлежность точки (пары чисел x и y) к данной группе определяется следующим соотношением:

$$y^2 \equiv x^3 + ax + b \pmod{p},$$

где модуль системы p является простым числом, большим 3, а a и b являются константами, удовлетворяющими следующим соотношениям: a, $b \in F_p$ и $4a^3 + 27b^2$ не сравнимо с нулем по модулю p.

При этом следует отметить, что принципы вычислений по данному алгоритму схожи с предшествующим отечественным стандартом ЭЦП: генерируется случайное число x, с его помощью вычисляется r-часть ЭЦП, затем вычисляется s-часть ЭЦП из r-части, x, значения секретного ключа и хэш-значения подписываемых данных. При проверке же подписи аналогичным вышеописанному образом проверяется соответствие определенным соотношениям r, s, открытого ключа и хэш-значения информации, подпись которой проверяется. Подпись считается неверной, если соотношения не соблюдаются. Математические подробности реализации этого алгоритма приводятся ниже.

Обозначения

В данном стандарте использованы следующие обозначения:

V_{256} — множество всех двоичных векторов длиной 256 бит;

V_∞ — множество всех двоичных векторов произвольной конечной длины;

Z — множество всех целых чисел;

p — простое число, $p > 3$;

F_p — конечное простое поле, представляемое как множество из p целых чисел $\{0, 1, ..., p-1\}$;

$b \pmod{p}$ — минимальное неотрицательное число, сравнимое с b по модулю p;

M — сообщение пользователя, $M \in V_\infty$;

$(\bar{h}_1 || \bar{h}_2)$ — конкатенация (объединение) двух двоичных векторов;

a, b — коэффициенты эллиптической кривой;

m — порядок группы точек эллиптической кривой;

q — порядок подгруппы группы точек эллиптической кривой;

O — нулевая точка эллиптической кривой;

P — точка эллиптической кривой порядка q;
d — целое число — ключ подписи;
Q — точка эллиптической кривой — ключ проверки;
w — цифровая подпись под сообщением M.

Общие положения

Механизм цифровой подписи реализуется посредством двух основных процессов:

- формирование цифровой подписи;
- проверка цифровой подписи.

В *процессе формирования цифровой подписи* в качестве исходных данных используются сообщение M, ключ подписи d и параметры схемы ЭЦП, а в результате формируется цифровая подпись w.

Ключ подписи d является элементом секретных данных, специфичным для субъекта и используемым только данным субъектом в процессе формирования цифровой подписи.

Параметры схемы ЭЦП — элементы данных, общие для всех субъектов схемы цифровой подписи, известные или доступные всем этим субъектам.

Электронная цифровая подпись w представляет собой строку битов, полученную в результате процесса формирования подписи. Данная строка имеет внутреннюю структуру, зависящую от конкретного механизма формирования подписи.

В *процессе проверки цифровой подписи* в качестве исходных данных используются подписанное сообщение, ключ проверки Q и параметры схемы ЭЦП, а результатом проверки является заключение о правильности или ошибочности цифровой подписи.

Ключ проверки Q является элементом данных, математически связанным с ключом подписи d и используемым проверяющей стороной в процессе проверки цифровой подписи.

Схематическое представление подписанного сообщения показано на рис. 4.23.

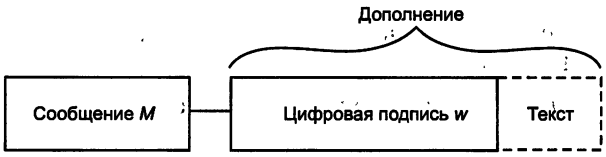


Рис. 4.23. Схема подписанного сообщения

Поле «Текст», показанное на рис. 4.23 и дополняющее поле «Цифровая подпись», может, например, содержать идентификаторы субъекта, подписавшего сообщение, и/или метку времени.

Установленная в данном стандарте схема цифровой подписи должна быть реализована с использованием операций группы точек эллип-

тической кривой, определенной над конечным простым полем, а также хэш-функции.

Криптографическая стойкость данной схемы цифровой подписи основывается на сложности решения задачи дискретного логарифмирования в группе точек эллиптической кривой, а также на стойкости используемой хэш-функции. Алгоритм вычисления хэш-функции установлен в ГОСТ Р 34.11.

Цифровая подпись, представленная в виде двоичного вектора длиной 512 бит, должна вычисляться и проверяться с помощью определенных наборов правил, изложенных ниже.

Параметры схемы цифровой подписи, необходимые для ее формирования и проверки:

- простое число p — модуль эллиптической кривой, — удовлетворяющее неравенству $p > 2^{255}$. Верхняя граница данного числа должна определяться при конкретной реализации схемы цифровой подписи;
- эллиптическая кривая E, задаваемая своим инвариантом $J(E)$ или коэффициентами $a, b \in F_p$;
- целое число m — порядок группы точек эллиптической кривой E;
- простое число q — порядок циклической подгруппы группы точек эллиптической кривой E, для которого выполнены следующие условия:

$$\begin{cases} m = nq, \ n \in Z, \ n \geq 1; \\ 2^{254} < q < 2^{256}; \end{cases}$$

- точка $P \neq 0$ эллиптической кривой E с координатами (x_p, y_p), удовлетворяющая равенству $qP = 0$;
- хэш-функция $h(\cdot): V_\infty \to V_{256}$, отображающая сообщения, представленные в виде двоичных векторов произвольной конечной длины, в двоичные векторы длиной 256 бит. Хэш-функция определена в ГОСТ Р 34.11.

Каждый пользователь схемы цифровой подписи должен обладать личными ключами:

- ключом подписи — целым числом d, удовлетворяющим неравенству $0 < d < q$;
- ключом проверки — точкой эллиптической кривой Q с координатами (x_q, y_q), удовлетворяющей равенству $dP = Q$.

На приведенные выше параметры схемы цифровой подписи накладываются следующие требования:

- должно быть выполнено условие $p^t \neq 1 \pmod p$ для всех целых $t = 1, 2, ..., B$, где B удовлетворяет неравенству $B \geq 31$;
- должно быть выполнено неравенство $m \neq p$;
- инвариант кривой должен удовлетворять условию $J(E) \neq 0$ или 1728.

Двоичные векторы

Для определения процессов формирования и проверки цифровой подписи необходимо установить соответствие между целыми числами и двоичными векторами длины 256 бит.

Рассмотрим следующий двоичный вектор длиной 256 бит, в котором младшие биты расположены справа, а старшие — слева:

$$\bar{h} = (\alpha_{255}, \ldots, \alpha_0), \quad \bar{h} \in V_{256},$$

где α_i, $i = 0$—256, равно либо 1, либо 0. Будем считать, что число $\alpha \in Z$ соответствует двоичному вектору $\bar{h}$, если выполнено равенство

$$\alpha = \sum_{i=0}^{255} \alpha_i 2^i.$$

Для двух двоичных векторов $\bar{h}_1$ и $\bar{h}_2$, соответствующих целым числам α и β, определим операцию конкатенации (объединения) следующим образом. Пусть

$$\bar{h}_1 = (\alpha_{255}, \ldots, \alpha_0);$$
$$\bar{h}_2 = (\beta_{255}, \ldots, \beta_0),$$

тогда их объединение имеет вид

$$\bar{h}_1 || \bar{h}_2 = (\alpha_{255}, \ldots, \alpha_0, \beta_{255}, \ldots, \beta_0)$$

и представляет собой двоичный вектор длиной 512 бит, составленный из коэффициентов векторов $\bar{h}_1$ и $\bar{h}_2$.

С другой стороны, приведенные формулы определяют способ разбиения двоичного вектора $\bar{h}$ длиной 512 бит на два двоичных вектора длиной 256 бит, конкатенацией которых он является.

Основные процессы

В данном разделе определены процессы формирования и проверки электронной цифровой подписи под сообщением пользователя.

Для реализации данных процессов необходимо, чтобы всем пользователям были известны параметры схемы цифровой подписи, удовлетворяющие приведенным выше требованиям.

Кроме того, каждый пользователь должен иметь ключ подписи d и ключ проверки подписи $Q(x_q, y_q)$, которые также должны удовлетворять приведенным выше требованиям.

Формирование цифровой подписи

Для получения цифровой подписи под сообщением $M \in V_\infty$ необходимо выполнить следующие действия (шаги).

Шаг 1. Вычислить хэш-код сообщения M: $\bar{h} = h(M)$.

Шаг 2. Вычислить целое число α, двоичным представлением которого является вектор $\bar{h}$, и определить значение $e \equiv \alpha \pmod{q}$. Если $e = 0$, то определить $e = 1$.

Шаг 3. Сгенерировать случайное (псевдослучайное) целое число k, удовлетворяющее неравенству $0 < k < q$.

Шаг 4. Вычислить точку эллиптической кривой $C = kP$ и определить $r \equiv x_c \pmod{q}$, где x_c — x-координата точки C. Если $r = 0$, то вернуться к шагу 3.

Шаг 5. Вычислить значение $s \equiv (rd + ke) \pmod{q}$. Если $s = 0$, то вернуться к шагу 3.

Шаг 6. Вычислить двоичные векторы $\bar{r}$ и $\bar{s}$, соответствующие r и s, и определить цифровую подпись $w = (\bar{r} \,||\, \bar{s})$ как конкатенацию двух двоичных векторов.

Исходными данными этого процесса являются ключ подписи d и подписываемое сообщение M, а выходным результатом — цифровая подпись w.

Проверка цифровой подписи

Для проверки цифровой подписи w под полученным сообщением M необходимо выполнить следующие действия (шаги).

Шаг 1. По полученной подписи w вычислить целые числа r и s. Если выполнены неравенства $0 < r < q$, $0 < s < q$, то перейти к следующему шагу. В противном случае подпись неверна.

Шаг 2. Вычислить хэш-код полученного сообщения M: $\bar{h} = h(M)$.

Шаг 3. Вычислить целое число α, двоичным представлением которого является вектор $\bar{h}$, и определить $e \equiv \alpha \pmod{q}$. Если $e = 0$, то определить $e = 1$.

Шаг 4. Вычислить значение $v \equiv e^{-1} \pmod{q}$.

Шаг 5. Вычислить значения $z_1 \equiv sv \pmod{q}$, $z_2 \equiv -rv \pmod{q}$.

Шаг 6. Вычислить точку эллиптической кривой $C = z_1P + z_2Q$ и определить $R \equiv x_c \pmod{q}$, где x_c — x-координата точки C.

Шаг 7. Если выполнено равенство $R = r$, то подпись принимается, в противном случае подпись неверна.

Исходными данными этого процесса являются подписанное сообщение M, цифровая подпись w и ключ проверки Q, а выходным результатом — свидетельство о достоверности или ошибочности данной подписи.

Внедрение цифровой подписи на базе стандарта ГОСТ Р 34.10—2001 повышает, по сравнению с предшествующей схемой цифровой подписи, уровень защищенности передаваемых сообщений от подделок и искажений. Этот стандарт рекомендуется использовать в новых системах обработки информации различного назначения, а также при модернизации действующих систем.

4.6. Управление криптоключами

Любая криптографическая система основана на использовании криптографических ключей. Под *ключевой информацией* понимают совокупность всех действующих в информационной сети или системе ключей. Если не обеспечено достаточно надежное управление ключевой информацией, то, завладев ею, злоумышленник получает неограниченный доступ ко всей информации в сети или системе. *Управление ключами* включает реализацию таких функций, как генерация, хранение и распределение ключей. *Распределение ключей* — самый ответственный процесс в управлении ключами.

При использовании симметричной криптосистемы две вступающие в информационный обмен стороны должны сначала согласовать секретный сессионный ключ, т. е. ключ для шифрования всех сообщений, передаваемых в процессе обмена. Этот ключ должен быть неизвестен всем остальным и должен периодически обновляться одновременно у отправителя и получателя. Процесс согласования сессионного ключа называют также обменом или распределением ключей.

Асимметричная криптосистема предполагает использование двух ключей — открытого и закрытого (секретного). Открытый ключ можно разглашать, а закрытый надо хранить в тайне. При обмене сообщениями необходимо пересылать только открытый ключ, обеспечив подлинность пересылаемого открытого ключа.

К распределению ключей предъявляются следующие требования:

- оперативность и точность распределения;
- конфиденциальность и целостность распределяемых ключей.

Для распределения ключей между пользователями компьютерной сети используются следующие основные способы [7]:

1. Использование одного или нескольких центров распределения ключей.
2. Прямой обмен ключами между пользователями сети.

Проблемой первого подхода является то, что центру распределения ключей известно, кому и какие ключи распределены, и это позволяет читать все сообщения, передаваемые по сети. Возможные злоупотребления могут существенно нарушить безопасность сети. При втором подходе проблема состоит в том, чтобы надежно удостовериться в подлинности субъектов сети.

Задача распределения ключей сводится к построению такого протокола распределения ключей, который обеспечивает:

- взаимное подтверждение подлинности участников сеанса;
- подтверждение достоверности сеанса;
- использование минимального числа сообщений при обмене ключами.

Характерным примером реализации первого подхода является система аутентификации и распределения ключей Kerberos. Система Kerberos рассмотрена в главе 12.

Остановимся подробнее на втором подходе — прямом обмене ключами между пользователями сети.

При использовании для защищенного информационного обмена криптосистемы с симметричным секретным ключом два пользователя, желающие обменяться криптографически защищенной информацией, должны обладать общим секретным ключом. Эти пользователи должны обменяться общим ключом по каналу связи безопасным образом. Если пользователи меняют ключ достаточно часто, то доставка ключа превращается в серьезную проблему.

Для решения этой проблемы можно применить два основных способа:

1. Использование асимметричной криптосистемы с открытым ключом для защиты секретного ключа симметричной криптосистемы.
2. Использование системы открытого распределения ключей Диффи — Хеллмана.

Реализация первого способа осуществляется в рамках комбинированной криптосистемы с симметричными и асимметричными ключами. При таком подходе симметричная криптосистема применяется для шифрования и передачи исходного открытого текста, а асимметричная криптосистема с открытым ключом — для шифрования, передачи и последующего расшифрования только секретного ключа симметричной криптосистемы.

Второй способ безопасного распространения секретных ключей основан на применении алгоритма открытого распределения ключей Диффи — Хеллмана. Этот алгоритм позволяет пользователям обмениваться ключами по незащищенным каналам связи.

4.6.1. Использование комбинированной криптосистемы

Анализ рассмотренных выше особенностей симметричных и асимметричных криптографических систем показывает, что при совместном использовании эти криптосистемы могут эффективно друг друга дополнить, компенсируя недостатки друг друга.

Действительно, главным достоинством асимметричных криптосистем с открытым ключом является их потенциально высокая безопасность: нет необходимости ни передавать, ни сообщать кому-либо значения секретных ключей, ни убеждаться в их подлинности. Однако быстродействие асимметричных криптосистем с открытым ключом обычно в сотни и более раз меньше быстродействия симметричных криптосистем с секретным ключом.

В свою очередь, быстродействующие симметричные криптосистемы страдают существенным недостатком: обновляемый секретный ключ симметричной криптосистемы должен регулярно передаваться партнерам по информационному обмену и во время этих передач возникает опасность раскрытия секретного ключа.

Совместное использование этих криптосистем позволяет эффективно реализовать такую базовую функцию защиты, как криптографическое закрытие передаваемой информации с целью обеспечения ее конфиденциальности.

Комбинированное применение симметричного и асимметричного шифрования позволяет устранить основные недостатки, присущие обоим методам. Комбинированный (гибридный) метод шифрования позволяет сочетать преимущества высокой секретности, предоставляемые асимметричными криптосистемами с открытым ключом, с преимуществами высокой скорости работы, присущими симметричным криптосистемам с секретным ключом.

Метод комбинированного использования симметричного и асимметричного шифрования заключается в следующем: симметричную криптосистему применяют для шифрования исходного открытого текста, а асимметричную криптосистему с открытым ключом — только для шифрования секретного ключа симметричной криптосистемы. В результате асимметричная криптосистема с открытым ключом не заменяет, а лишь дополняет симметричную криптосистему с секретным ключом, позволяя повысить в целом защищенность передаваемой информации. Такой подход иногда называют схемой *электронного цифрового конверта.*

Пусть пользователь *A* хочет использовать комбинированный метод шифрования для защищенной передачи сообщения *M* пользователю *B.*

Тогда последовательность действий пользователей *A* и *B* будет следующей.

Действия пользователя A:

1. Создает (например, генерирует случайным образом) сеансовый секретный ключ K_S, который будет использован в алгоритме симметричного шифрования для зашифрования конкретного сообщения или цепочки сообщений.

2. Зашифровывает симметричным алгоритмом сообщение *M* на сеансовом секретном ключе K_S.

3. Зашифровывает асимметричным алгоритмом секретный сеансовый ключ K_S на открытом ключе K_B пользователя *B* (получателя сообщения).

4. Передает по открытому каналу связи в адрес пользователя *B* зашифрованное сообщение *M* вместе с зашифрованным сеансовым ключом K_S.

Действия пользователя *A* иллюстрируются схемой шифрования сообщения комбинированным методом (рис. 4.24).

Действия пользователя B (при получении электронного цифрового конверта — зашифрованного сообщения *M* и зашифрованного сеансового ключа K_S):

5. Расшифровывает асимметричным алгоритмом сеансовый ключ K_S с помощью своего секретного ключа k_B.

6. Расшифровывает симметричным алгоритмом принятое сообщение *M* с помощью полученного сеансового ключа K_S.

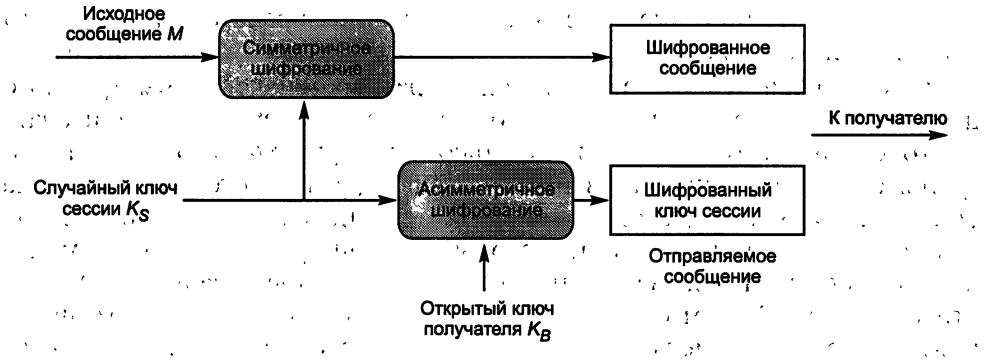


Рис. 4.24. Схема шифрования сообщения комбинированным методом

Действия пользователя *B* иллюстрируются схемой расшифрования сообщения комбинированным методом (рис. 4.25).

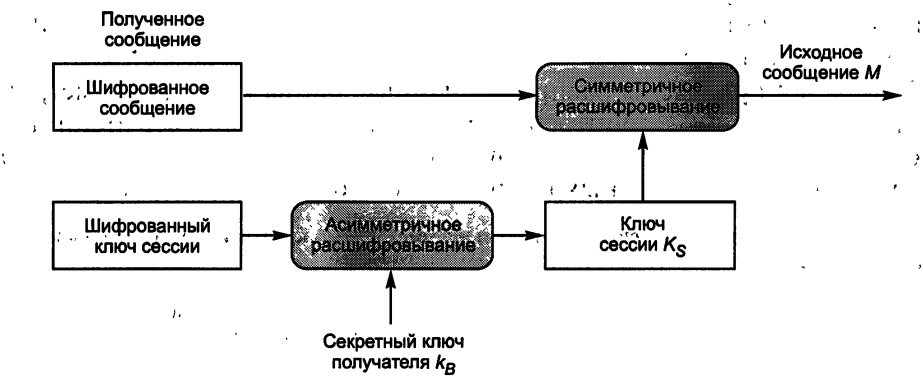


Рис. 4.25. Схема расшифрования сообщения комбинированным методом

Полученный электронный цифровой конверт может раскрыть только законный получатель — пользователь *B*. Только пользователь *B*, владеющий личным секретным ключом k_B, сможет правильно расшифровать секретный сеансовый ключ K_S и затем с помощью этого ключа расшифровать и прочитать полученное сообщение *M*.

При методе цифрового конверта недостатки симметричного и асимметричного криптоалгоритмов компенсируются следующим образом:

- проблема распространения ключей симметричного криптоалгоритма устраняется тем, что сеансовый ключ K_S, на котором шифруются собственно сообщения, передается по открытым каналам связи в зашифрованном виде; для зашифрования ключа K_S используется асимметричный криптоалгоритм;
- проблемы медленной скорости асимметричного шифрования в данном случае практически не возникает, поскольку асимметричным криптоалгоритмом шифруется только короткий ключ K_S, а все данные шифруются быстрым симметричным криптоалгоритмом.

В результате получают быстрое шифрование в сочетании с удобным распределением ключей.

С целью защиты от разглашения секретных ключей симметричного шифрования любой из сторон обмена, когда требуется реализовать протоколы взаимодействия не доверяющих друг другу сторон, используется следующий способ взаимодействия. Для каждого сообщения на основе случайных параметров генерируется отдельный секретный ключ симметричного шифрования, который и зашифровывается асимметричной системой для передачи вместе с сообщением, зашифрованным этим ключом. В этом случае разглашение ключа симметричного шифрования не будет иметь смысла, так как для зашифровывания следующего сообщения будет использован другой случайный секретный ключ.

При комбинированном методе шифрования применяются криптографические ключи как симметричных, так и асимметричных криптосистем. Очевидно, выбор длин ключей для криптосистемы каждого типа следует осуществлять таким образом, чтобы злоумышленнику было одинаково трудно атаковать любой механизм защиты комбинированной криптосистемы.

В табл. 4.4 приведены распространенные длины ключей симметричных и асимметричных криптосистем, для которых трудность атаки полного перебора примерно равна трудности факторизации соответствующих модулей асимметричных криптосистем [63].

Таблица 4.4. **Длины ключей для симметричных и асимметричных криптосистем при одинаковой их криптостойкости**

Длина ключа симметричной криптосистемы, бит	Длина ключа асимметричной криптосистемы, бит
56	384
64	512
80	768
112	1792
128	2304

Если используется короткий сеансовый ключ (например, 56-битный ключ алгоритма DES), то не имеет значения, насколько велики асимметричные ключи. Злоумышленник будет атаковать не их, а сеансовый ключ.

4.6.2. Метод распределения ключей Диффи — Хеллмана

У. Диффи и М. Хеллман изобрели метод *открытого распределения ключей* в 1976 г. Этот метод позволяет пользователям обмениваться ключами по незащищенным каналам связи. Его безопасность обусловлена трудностью вычисления дискретных логарифмов в конечном поле,

в отличие от легкости решения прямой задачи дискретного возведения в степень в том же конечном поле.

Суть метода Диффи — Хеллмана заключается в следующем (рис. 4.26).

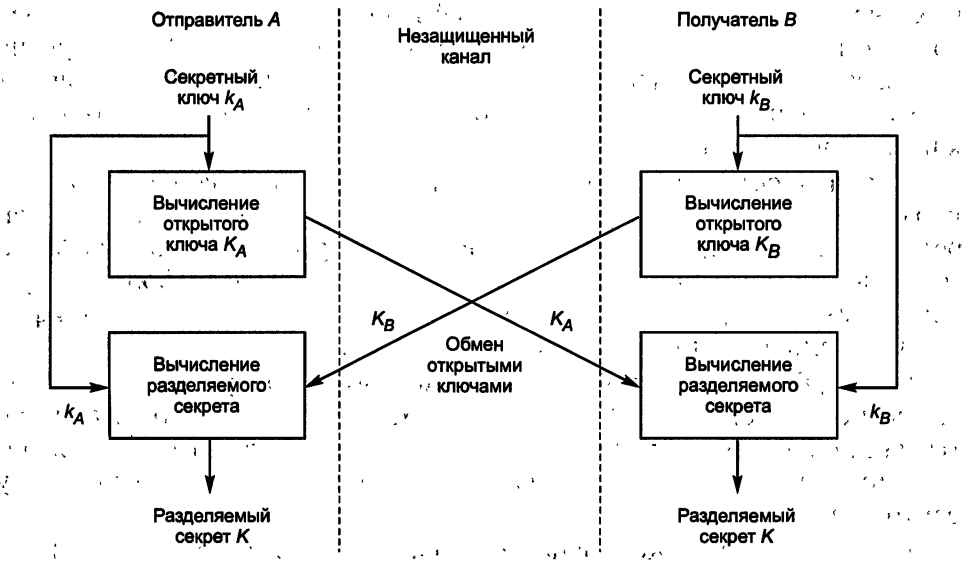


Рис. 4.26. Схема открытого распределения ключей Диффи — Хеллмана

Пользователи A и B, участвующие в обмене информации, генерируют независимо друг от друга свои случайные секретные ключи k_A и k_B (ключи k_A и k_B — случайные большие целые числа, которые хранятся пользователями A и B в секрете).

Затем пользователь A вычисляет на основании своего секретного ключа k_A открытый ключ

$$K_A = g^{k_A} \pmod N.$$

Одновременно пользователь B вычисляет на основании своего секретного ключа k_B открытый ключ

$$K_B = g^{k_B} \pmod N,$$

где N и g — большие целые простые числа. Арифметические действия выполняются с приведением по модулю N [63]. Числа N и g могут не храниться в секрете. Как правило, эти значения являются общими для всех пользователей сети или системы.

Затем пользователи A и B обмениваются своими открытыми ключами K_A и K_B по незащищенному каналу и используют их для вычисления общего сессионного ключа K (разделяемого секрета):

- пользователь A: $K = (K_B)^{k_A} \pmod N = (g^{k_B})^{k_A} \pmod N$;
- пользователь B: $K' = (K_A)^{k_B} \pmod N = (g^{k_A})^{k_B} \pmod N$;
- при этом $K = K'$, так как $(g^{k_B})^{k_A} = (g^{k_A})^{k_B} \pmod N$.

Таким образом, результатом этих действий оказывается общий сессионный ключ, который является функцией обоих секретных ключей k_A и k_B.

Злоумышленник, перехвативший значения открытых ключей K_A и K_B, не может вычислить сессионный ключ K, потому что он не имеет соответствующих значений секретных ключей k_A и k_B. Благодаря использованию однонаправленной функции операция вычисления открытого ключа необратима, т. е. невозможно по значению открытого ключа абонента вычислить его секретный ключ.

Уникальность метода Диффи — Хеллмана заключается в том, что пара абонентов имеет возможность получить известное только им секретное число, передавая по открытой сети открытые ключи. После этого абоненты могут приступить к защите передаваемой информации уже известным проверенным способом — применяя симметричное шифрование с использованием полученного разделяемого секрета.

Схема Диффи — Хеллмана дает возможность шифровать данные при каждом сеансе связи на новых ключах. Это позволяет не хранить секреты на дискетах или других носителях. Не следует забывать, что любое хранение секретов повышает вероятность попадания их в руки конкурентов или противника.

Схема Диффи — Хеллмана позволяет реализовать *метод комплексной защиты конфиденциальности и аутентичности передаваемых данных.* Эта схема предоставляет пользователям возможность сформировать и использовать одни и те же ключи для выполнения цифровой подписи и симметричного шифрования передаваемых данных.

Метод комплексной защиты конфиденциальности и аутентичности передаваемых данных

Для одновременной защиты целостности и конфиденциальности данных целесообразно применять шифрование и электронную цифровую подпись в комплексе. Промежуточные результаты работы схемы Диффи — Хеллмана могут быть использованы в качестве исходных данных для реализации метода комплексной защиты целостности и конфиденциальности передаваемых данных [45].

Действительно, согласно данному алгоритму пользователи A и B сначала генерируют свои секретные ключи k_A и k_B и вычисляют свои открытые ключи K_A и K_B. Затем абоненты A и B используют эти промежуточные результаты для одновременного вычисления общего разделяемого секретного ключа K, который может использоваться для симметричного шифрования данных.

Метод комплексной защиты конфиденциальности и аутентичности передаваемых данных работает по следующей схеме:

- абонент A подписывает сообщение M с помощью своего секретного ключа k_A, используя стандартный алгоритм цифровой подписи;

- абонент A вычисляет совместно разделяемый секретный ключ K по алгоритму Диффи — Хеллмана из своего секретного ключа k_A и открытого ключа K_B абонента B;
- абонент A зашифровывает сообщение M на полученном совместно разделяемом секретном ключе K, используя согласованный с партнером по обмену алгоритм симметричного шифрования;
- абонент B при получении зашифрованного сообщения M вычисляет по алгоритму Диффи — Хеллмана совместно разделяемый секретный ключ K из своего секретного ключа k_B и открытого ключа K_A абонента A;
- абонент B расшифровывает полученное сообщение M на ключе K;
- абонент B проверяет подпись расшифрованного сообщения M с помощью открытого ключа абонента K_A.

На основе схемы Диффи — Хеллмана функционируют протоколы управления криптоключами SKIP (Simple Key management for Internet Protocols) и IKE (Internet Key Exchange), применяемые при построении защищенных виртуальных сетей VPN на сетевом уровне.

4.6.3. Протокол вычисления ключа парной связи ECKEP

В протоколе вычисления ключа эллиптической кривой ECKEP (Elliptic Curve Key Establishment Protocol) определение параметров системы и генерация ключей аналогичны алгоритму асимметричного шифрования ECES.

Предположим, что общий ключ вычисляется пользователями A и B.

Пользователь A имеет секретный ключ a и открытый ключ $Q_A = aP = (x_A, y_A)$. Аналогично пользователь B имеет секретный ключ b и открытый ключ $Q_B = bP = (x_B, y_B)$.

Вычисление ключа парной связи производится в четыре этапа.

Этап 1. Действия пользователя A:

- выбирается случайное целое число k_A, $1 \le k_A \le n - 1$;
- вычисляется точка $R_A = k_A P$;
- вычисляется точка $(x_1, y_1) = k_A Q_B$;
- вычисляется $s_A = k_A + a x_A x_1 \bmod n$;
- R_A отправляется пользователю B.

Этап 2. Действия пользователя B:

- выбирается случайное целое число k_B, $1 \le k_B \le n - 1$;
- вычисляется точка $R_B = k_B P$;
- вычисляется точка $(x_2, y_2) = k_B Q_A$;
- вычисляется $s_B = k_B + b x_B x_2 \bmod n$;
- R_B отправляется пользователю A.

Этап 3. Действия пользователя A:

- вычисляется $(x_2, y_2) = aR_B$;
- вычисляется ключ парной связи $K = s_A(R_B + x_B x_2 Q_B)$.

Этап 4. Действия пользователя B:

- вычисляется $(x_1, y_1) = bR_A$;
- вычисляется ключ парной связи $K = s_B(R_A + x_A x_1 Q_A)$, что эквивалентно значению $s_A(R_B + x_B x_2 Q_B)$.

Важным достоинством схемы распределения ключей Диффи — Хеллмана и протокола вычисления ключа парной связи ECKEP является то, что они позволяют обойтись без защищенного канала для передачи ключей. Однако необходимо иметь гарантию того, что пользователь *A* получил открытый ключ именно от пользователя *B*, и наоборот. Эта проблема решается с помощью сертификатов открытых ключей, создаваемых и распространяемых центрами сертификации CA (Certification Authority) в рамках инфраструктуры управления открытыми ключами PKI (Public Key Infrastructure).

4.7. Инфраструктура управления открытыми ключами PKI

Исторически в обязанности любого центра управления информационной безопасностью всегда входил набор задач по управлению ключами, используемыми различными средствами защиты информации (СЗИ). В этот набор входят выдача, обновление, отмена и распространение ключей.

В случае использования симметричной криптографии задача распространения секретных ключей представляла наиболее сложную проблему, поскольку:

- необходимо для *N* пользователей распространять в защищенном режиме $N(N-1)/2$ ключей, что при *N* порядка нескольких сотен может стать очень обременительной задачей;
- система распространения ключей получается сложной (много ключей и закрытый канал распространения), что приводит к появлению уязвимых мест.

Асимметричная криптография позволяет обойти эту проблему, предложив к использованию только *N* секретных ключей. При этом у каждого пользователя только один секретный ключ и один открытый, полученный по специальному алгоритму из секретного.

Из открытого ключа практически невозможно получить секретный, поэтому открытый ключ можно распространять открытым способом всем участникам взаимодействия. На основании своего закрытого ключа и открытого ключа своего партнера по взаимодействию любой участник может выполнять любые криптографические операции: генерацию электронно-цифровой подписи, расчет разделяемого секрета, защиту конфиденциальности и целостности сообщения.

В результате решаются две главные проблемы симметричной криптографии:

- перегруженность количеством ключей — их теперь всего *N*;
- сложность распространения — их можно распространять открыто.

Однако у этой технологии есть один недостаток — подверженность атаке «человек-в-середине», когда атакующий злоумышленник расположен между участниками взаимодействия. В этом случае появляется риск подмены передаваемых открытых ключей.

Инфраструктура управления открытыми ключами PKI позволяет преодолеть этот недостаток и обеспечить эффективную защиту от атаки «человек-в-середине».

4.7.1. Принципы функционирования PKI

Инфраструктура открытых ключей PKI (Public Key Infrastructure) предназначена для надежного функционирования корпоративных информационных систем и позволяет как внутренним, так и внешним пользователям безопасно обмениваться информацией с помощью цепочки доверительных отношений. Инфраструктура открытых ключей PKI основывается на цифровых сертификатах, которые действуют подобно электронным паспортам, связывающим индивидуальный секретный ключ пользователя с его открытым ключом.

Защита от атаки «человек-в-середине»

При осуществлении атаки «человек-в-середине» атакующий может незаметно подменить передаваемые по открытому каналу открытые ключи законных участников взаимодействия на свой открытый ключ, создать разделяемые секреты с каждым из законных участников и затем перехватывать и расшифровывать все их сообщения.

Поясним на примере действия атакующего злоумышленника (рис. 4.27). Предположим, есть два пользователя i и j, каждый из которых имеет по паре ключей, при этом у пользователя j есть открытый

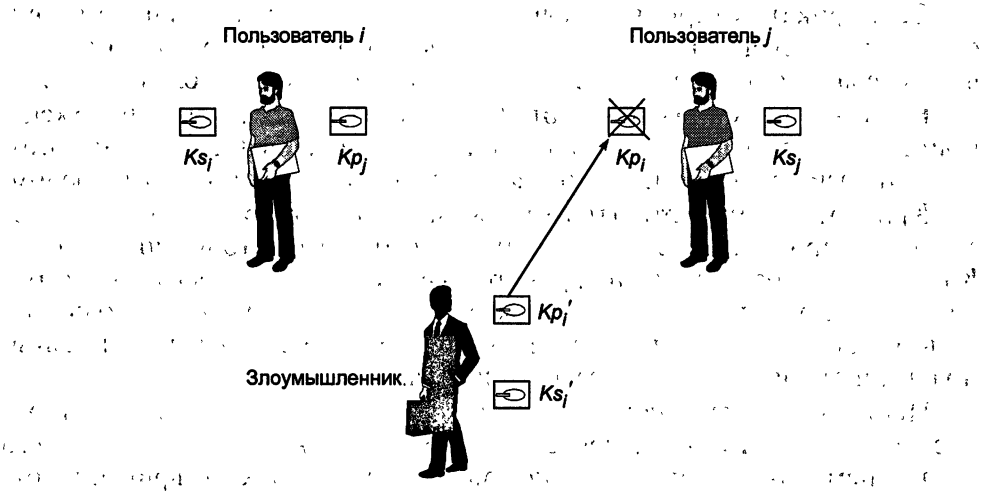


Рис. 4.27. Подмена открытого ключа

ключ Kp_i для проверки ЭЦП пользователя i. Далее предположим, что злоумышленник может перехватить этот ключ Kp_i в процессе его передачи от пользователя i пользователю j или получить доступ к этому ключу, хранящемуся у пользователя j. В любом случае злоумышленник считает из ключа его реквизиты (например, фамилию владельца, место работы и т. д.) и создаст свою пару ключей, Ks_i' и Kp_i', в которые запишет известные ему реквизиты пользователя i. Затем он подменит посланный пользователю j открытый ключ Kp_i своим фальшивым открытым ключом Kp_i', имеющим реквизиты пользователя i.

Любое сообщение злоумышленник будет подписывать своим секретным ключом Ks_i' (причем для пользователя j эта подпись выглядит так, как если бы она была поставлена пользователем i). Подпись такого сообщения, проверяемая пользователем j, будет верна, поскольку ему был послан фальшивый ключ Kp_i', парный столь же фальшивому ключу Ks_i'.

Подмена открытого ключа раскроется только после того, как настоящий пользователь i пошлет пользователю j сообщение, подписанное истинным ключом Ks_i. Но ситуация может находиться под контролем злоумышленника достаточно долго, тем более что он вполне может заранее оценить необходимое время сеансов связи, проанализировав интенсивность документооборота между пользователями i и j, а также рассчитать время, в течение которого подмена ключа не будет обнаружена. Проблема также существенно усугубляется, если злоумышленник имеет техническую возможность перехватывать сообщения, посылаемые пользователем i пользователю j.

Описанная угроза подмены открытых ключей успешно устраняется путем использования сертификатов открытых ключей.

Сертификаты открытых ключей

Сертификаты открытых ключей играют важную роль в криптографии открытых ключей. Основное назначение сертификата открытого ключа — сделать доступным и достоверным открытый ключ пользователя.

В основу формирования сертификатов открытых ключей положены принципы строгой аутентификации, рекомендованные стандартом X.509 и базирующиеся на свойствах криптосистем с открытым ключом.

Криптосистемы с открытым ключом предполагают наличие у пользователя парных ключей — секретного и открытого (общедоступного). Каждый пользователь идентифицируется с помощью своего секретного ключа. С помощью парного открытого ключа любой другой пользователь имеет возможность определить, является ли его партнер по связи подлинным владельцем секретного ключа.

Процедура, позволяющая каждому пользователю устанавливать однозначное и достоверное соответствие между открытым ключом и его владельцем, обеспечивается с помощью механизма сертификации открытых ключей.

Степень достоверности факта установления подлинности (аутентификации) пользователя зависит от надежности хранения секретного ключа и надежности источника поставки открытых ключей пользователей. Чтобы пользователь мог доверять процессу аутентификации, он должен извлекать открытый ключ другого пользователя из надежного источника, которому он доверяет.

Таким источником согласно стандарту X.509 является *центр сертификации CA (Certification Authority)*. Центр сертификации называют также УЦ — *удостоверяющим центром*; последний термин используется, в частности, в отечественном «Законе об ЭЦП» [58].

Центр сертификации CA является *доверенной третьей стороной*, которая обеспечивает аутентификацию открытых ключей, содержащихся в сертификатах. CA имеет собственную пару ключей (открытый/секретный), где секретный ключ CA используется для подписывания сертификатов, а открытый ключ CA публикуется и применяется пользователями для проверки подлинности открытого ключа, содержащегося в сертификате.

Сертификация открытого ключа — это подтверждение подлинности открытого ключа и хранимой совместно с ним служебной информации, в частности, о принадлежности ключа. Сертификация ключа выполняется путем вычисления ЭЦП сертифицируемого ключа и служебной информации с помощью специального секретного ключа-сертификата, доступного только центру сертификации CA. Иными словами, сертификация открытого ключа — это подписывание открытого ключа электронной подписью, вычисленной на секретном ключе центра сертификации.

Открытый ключ совместно с сертифицирующей его ЭЦП часто называют *сертификатом открытого ключа* или просто *сертификатом*.

Открытый ключ сертификационного центра (парный секретному, на котором проводится сертификация других открытых ключей) используется для проверки целостности сертифицированных открытых ключей. Его обычно называют *ключом-сертификатом*.

Центр сертификации CA формирует сертификат открытого ключа пользователя путем заверения цифровой подписью CA определенного набора данных.

В соответствии с форматом X.509 в этот набор данных включаются:

- период действия открытого ключа, состоящий из двух дат: начала и конца периода;
- номер и серия ключа;
- уникальное имя пользователя;
- информация об открытом ключе пользователя: идентификатор алгоритма, для которого предназначен данный ключ, и собственно открытый ключ;
- ЭЦП и информация, используемая при проведении процедуры проверки ЭЦП (например, идентификатор алгоритма генерации ЭЦП);
- уникальное имя сертификационного центра.

Таким образом, цифровой сертификат содержит три главные составляющие:

- информацию о пользователе-владельце сертификата;
- открытый ключ пользователя;
- сертифицирующую ЭЦП двух предыдущих составляющих, вычисленную на секретном ключе CA.

Сертификат открытого ключа обладает следующими свойствами:

- каждый пользователь, имеющий доступ к открытому ключу центра сертификации CA, может извлечь открытый ключ, включенный в сертификат;
- ни одна сторона, помимо центра сертификации, не может изменить сертификат так, чтобы это не было обнаружено (сертификаты нельзя подделать).

Так как сертификаты не могут быть подделаны, их можно опубликовать, поместив в общедоступный справочник и не предпринимая специальных усилий по их защите.

Создание сертификата открытого ключа начинается с создания пары ключей (открытый/секретный).

Процедура генерации ключей может осуществляться двумя способами:

1. CA создает пару ключей. Открытый ключ заносится в сертификат, а парный ему секретный ключ передается пользователю с обеспечением аутентификации пользователя и конфиденциальности передачи ключа.

2. Пользователь сам создает пару ключей. Секретный ключ сохраняется у пользователя, а открытый ключ передается по защищенному каналу в CA.

Каждый пользователь может быть владельцем одного или нескольких сертификатов, сформированных сертификационным центром CA пользователя. Пользователь может владеть сертификатами, полученными из нескольких разных сертификационных центров.

4.7.2. Логическая структура и компоненты PKI

Инфраструктура открытых ключей PKI (Public Key Infrastructure) — это набор программных агентов и правил, предназначенных для управления ключами, политикой безопасности и собственно обменом защищенными сообщениями [7, 45].

Основными задачами PKI являются:

- поддержка жизненного цикла цифровых ключей и сертификатов (т. е. генерация ключей, создание и подпись сертификатов, их распределение и пр.);
- регистрация фактов компрометации и публикация черных списков отозванных сертификатов;
- поддержка процессов идентификации и аутентификации пользователей таким образом, чтобы сократить по возможности время допуска каждого пользователя в систему;

- реализация механизма интеграции (основанного на PKI) существующих приложений и всех компонентов подсистемы безопасности;
- предоставление возможности использования единственного токена безопасности, единообразного для всех пользователей и приложений и содержащего все необходимые ключевые компоненты и сертификаты.

Токен безопасности — это индивидуальное средство безопасности, определяющее все права и окружение пользователя в системе, например USB-ключ или смарт-карта.

Приложение, требующее систему управления ключами, должно взаимодействовать с системой PKI в целом ряде точек (передача сертификата на подпись, получение сертификата и черного списка при установлении взаимодействия и т. п.). Очевидно, что это взаимодействие с чужой по отношению к данному приложению системой может осуществляться только при условии полной поддержки международных стандартов, которым удовлетворяет большинство современных PKI-систем (например, Baltimore, Entrust, Verisign).

Для предоставления удаленного доступа мобильным пользователям центр управления должен допускать подключение компьютеров, IP-адрес которых ему заранее неизвестен. Участники информационного обмена опознаются по их криптографическим сертификатам. Так как криптографический сертификат пользователя является электронным паспортом, он, как и любой паспорт, должен соответствовать определенным стандартам. В криптографии это стандарт X.509.

Концепция инфраструктуры открытых ключей PKI подразумевает, что все сертификаты конкретной PKI (своя PKI может быть у любой организации или организационной единицы) организованы в иерархическую структуру. Пример иерархии сертификатов двух PKI показан на рис. 4.28.

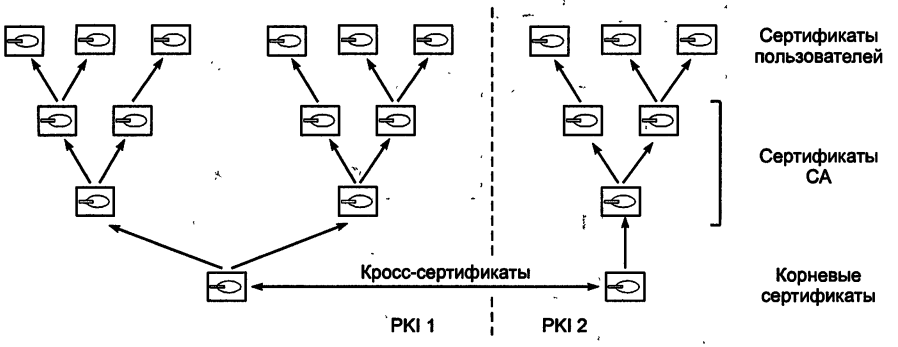


Рис. 4.28. Иерархическая структура сертификатов

Иерархическая схема PKI предусматривает существование четырех типов сертификатов:

1. *Сертификат конечного пользователя* (описанный выше).
2. *Сертификат CA.* Должен быть доступен для проверки ЭЦП сертификата конечного пользователя и подписан секретным ключом CA

верхнего уровня, причем эта ЭЦП также должна проверяться, для чего должен быть доступен сертификат СА верхнего уровня, и т. д.

3. *Самоподписанный сертификат.* Является *корневым* для всей PKI и доверенным по определению. Если в результате проверки цепочки сертификатов СА выяснится, что один из них подписан корневым секретным ключом, тогда процесс проверки ЭЦП сертификатов заканчивается.

4. *Кросс-сертификат.* Кросс-сертификаты позволяют расширить действие конкретной PKI путем взаимоподписания корневых сертификатов двух разных PKI.

Процедура проверки ЭЦП электронного документа происходит в системе PKI следующим образом. Сначала проверяется ЭЦП конкретного документа, а затем — ЭЦП сертификата, с помощью которого проверялась предыдущая ЭЦП. Последняя проверка повторяется в цикле до тех пор, пока цепочка сертификатов не приведет к корневому. ЭЦП документа признается верной лишь в том случае, если верна не только она, но и все проверяемые в данном процессе ЭЦП сертификатов. При обнаружении неверной ЭЦП любого из сертификатов неверными считаются все ЭЦП, проверенные на предыдущих шагах.

Заметим, что корневых сертификатов может быть несколько: каждая организация (или организационная единица) вправе устанавливать свои корневые сертификаты (один или несколько). Стандартом предусмотрено и наличие корневого сертификата для всего сообщества пользователей Интернета.

Логическая структура и основные компоненты инфраструктуры управления открытыми ключами PKI приведены на рис. 4.29.

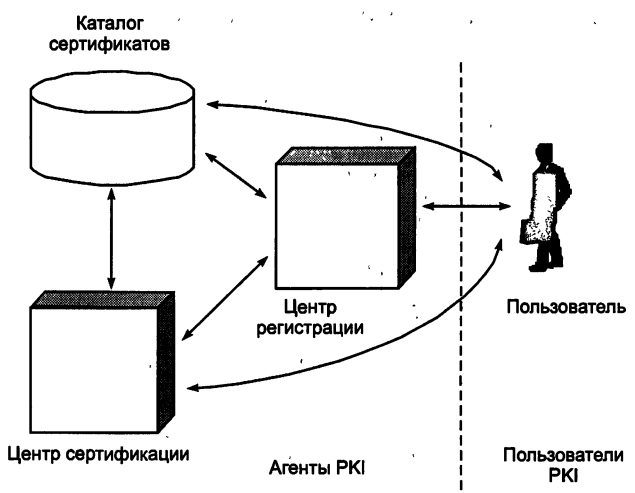


Рис. 4.29. Структура PKI

Компоненты этой структуры имеют следующее назначение.

Каталог сертификатов — общедоступное хранилище сертификатов пользователей. Доступ к сертификатам производится обычно по стан-

дартизованному протоколу доступа к каталогам LDAP (Lightweight Directory Access Protocol).

Центр регистрации RA *(Registration Authority)* — организационная единица, назначение которой — регистрация пользователей системы.

Пользователь — владелец какого-либо сертификата (такой пользователь подлежит регистрации) или любой пользователь, запрашивающий сертификат, хранящийся в каталоге сертификатов.

Центр сертификации CA *(Certification Authority)* — организационная единица, назначение которой — сертификация открытых ключей пользователей (здесь из открытого ключа получается сертификат формата X.509) и их опубликование в каталоге сертификатов.

Общая схема работы центра сертификации CA выглядит следующим образом:

- CA генерирует собственные ключи и формирует сертификаты CA, предназначенные для проверки сертификатов пользователей;
- пользователи формируют запросы на сертификацию и доставляют их CA тем или иным способом;
- CA на основе запросов пользователей формирует сертификаты пользователей;
- CA формирует и периодически обновляет списки отмененных сертификатов CRL (Certificate Revocation List);
- сертификаты пользователей, сертификаты CA и списки отмены CRL публикуются CA (рассылаются пользователям либо помещаются в общедоступный справочник).

Функции, выполняемые PKI в целом, можно условно разделить на несколько групп:

- функции управления сертификатами;
- функции управления ключами;
- дополнительные функции (службы).

Кратко рассмотрим эти основные группы функций.

В состав *функций управления сертификатами* входят:

- *регистрация пользователей.* Пользователем может быть физический пользователь, прикладная программа, сетевое устройство и пр.;
- *сертификация открытых ключей.* По существу, процесс сертификации состоит в связывании имени пользователя и открытого ключа. CA подписывает сертификаты пользователей и CA более низкого уровня;
- *сохранение закрытого ключа CA.* Это главная болевая точка системы. Компрометация закрытого ключа CA разрушает всю систему;
- *содержание базы сертификатов и их распределение.* Все сертификаты пользователей и промежуточных CA (кроме CA самого верхнего уровня!) обычно выкладываются на общедоступный сервер — сервер сертификатов;
- *обновление сертификата.* Процесс активизируется в случае истечения срока действия сертификата и состоит в передаче нового сертификата для открытого ключа пользователя;

- *обновление ключей.* При генерации новой пары ключей пользователем либо третьей стороной необходима генерация нового сертификата;
- *отзыв сертификата.* Этот процесс возможен, например, при компрометации ключей, изменении имени, прекращении доступа и пр.;
- *определение статуса отзыва сертификата.* Пользователь проверяет наличие сертификата в каталоге открытых ключей PKD (Public Key Directory) и в списке отзыва сертификатов CRL.

Функции управления ключами делятся на следующие основные подгруппы:

- генерация ключей;
- распределение ключей.

В состав группы *дополнительных функций (служб)* входят:

- взаимная сертификация (кросс-сертификация в различных CA);
- проверка открытого ключа с целью убедиться в соответствии открытого ключа арифметическим требованиям для таких ключей;
- проверка сертификата по просьбе пользователя;
- служба архивирования и др.

Взаимодействие компонентов инфраструктуры открытых ключей

В состав системы управления инфраструктурой открытых ключей могут входить дополнительные компоненты:

- модули интеграции — программные агенты для прикладных и клиентских систем, программные интерфейсы к сетевым приложениям и веб-сервисам;
- средства хранения ключевой информации и сертификатов пользователя — чаще всего в качестве таких средств выступают аппаратные токены, смарт-карты, USB-ключи.

Интеграция компонентов инфраструктуры открытых ключей со службой каталога позволяет автоматизировать множество задач, связанных с управлением PKI:

- автоматическое создание сертификатов для объектов каталога, управляемое политиками;
- автоматическая публикация списков отозванных сертификатов и сертификатов CA.

Кроме того, служба каталога может служить доверенным источником информации о сертификатах других участников криптографического обмена.

Физически система управления инфраструктурой открытых ключей может состоять из нескольких уровней:

- корневой узел в составе центра сертификации, хранилища сертификатов (служба каталогов) и средств администрирования;
- периферийный узел, включающий центр регистрации, используется при географической распределенности подразделений организации и большом количестве пользователей;

- клиентские станции с необходимыми программными компонентами.

Система управления инфраструктурой открытых ключей и ее компоненты являются основой для создания ряда подсистем комплексной системы обеспечения безопасности организации:

- *подсистема управления жизненным циклом отчуждаемых ключевых носителей* — подсистема, предназначенная для управления и учета аппаратных средств аутентификации пользователей (USB-ключей и смарт-карт) в масштабах предприятия. Эта подсистема является связующим звеном между пользователями, средствами аутентификации, приложениями информационной безопасности и корпоративной политикой безопасности;
- *подсистема генерации ключей шифрования и ЭЦП*, используемая для:
  - создания систем юридически значимой электронной цифровой подписи в системах электронного документооборота (в соответствии с Федеральным законом РФ об электронной цифровой подписи № 1-ФЗ от 10.01.2002);
  - реализации систем однократной и многофакторной аутентификации при доступе к автоматизированным информационным системам;
- *подсистема безопасного хранения и управления ключевой информацией*, реализующая следующие функции:
  - контроль целостности электронных документов;
  - контроль целостности публичных информационных ресурсов;
  - проверку подлинности взаимодействующих программных компонентов и конфиденциальности передаваемых данных при информационном взаимодействии;
  - обеспечение безопасности и разграничение доступа при взаимодействии субъектов автоматизированных информационных систем;
- *подсистема защищенного проставления меток времени*, формирующая штампы времени в электронном документообороте, что позволяет создавать доказательство факта существования документа на определенный момент времени.

На рис. 4.30 приведена схема инфраструктуры открытых ключей на базе продуктов Microsoft Active Directory и Microsoft Certification Authority. Удостоверяющие центры образуют в приведенном решении двухуровневую иерархию.

Изолированный корневой удостоверяющий центр физически отключен от сети. Этот удостоверяющий центр издает сертификаты только для нижестоящих УЦ. Применение изолированного корневого УЦ позволяет уменьшить риск компрометации всей инфраструктуры открытых ключей в случае успешной атаки на УЦ.

Издающий удостоверяющий центр в данном решении интегрирован в среду MS Active Directory, что позволяет ему автоматически публиковать списки отозванных сертификатов в службе каталога, а также автоматически обслуживать клиентов Active Directory.

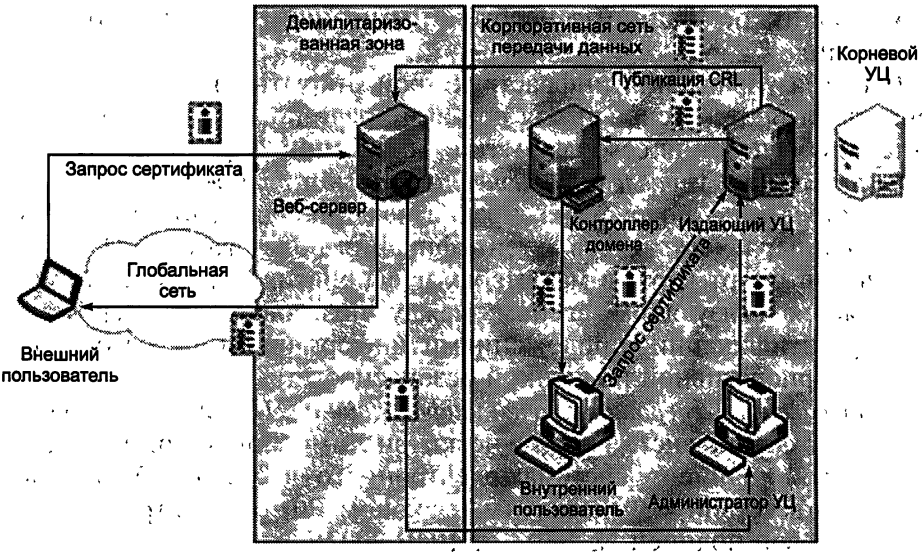


Рис. 4.30. Схема инфраструктуры открытых ключей на базе продуктов Microsoft Active Directory и Microsoft Certification Authority

Публикация списков отозванных сертификатов производится как в службу каталога, так и на корпоративный веб-сервер (для внешних клиентов, не имеющих доступ к службе каталога организации).

Инфраструктуру открытых ключей PKI поддерживает ряд приложений и стандартов, к ним можно отнести следующие:

- операционные системы Linux, FreeBSD, HP-UX, Microsoft Windows, Novell Netware, Sun Solaris, в которые встроены средства, поддерживающие сертификаты открытых ключей;
- системы управления базами данных, в частности Oracle, DB2, Informix, Sybase, которые поддерживают механизмы аутентификации пользователей на основе сертификатов открытых ключей;
- средства организации виртуальных защищенных сетей VPN, реализуемые на основе протокола IPSec, в частности телекоммуникационное оборудование компаний Cisco Systems, Nortel Network, а также специализированное программное обеспечение;
- системы электронного документооборота, например Lotus Notes, Microsoft Exchange, а также почтовые системы, поддерживающие стандарт защищенного почтового обмена S/MIME;
- службы каталогов Microsoft Active Directory, Novell NDS, Netscape iPlanet;
- системы доступа к веб-ресурсам, реализуемые на основе стандарта SSL;
- системы аутентификации пользователей, в частности система SecurId компании RSA и др.

В свою очередь, инфраструктура открытых ключей PKI может интегрировать перечисленные функциональные области. В результате можно создавать комплексную систему информационной безопасности

путем интеграции инфраструктуры открытых ключей в информационную систему компании и использования единых стандартов и сертификатов открытых ключей.

Вопросы для самоконтроля

1. Что такое криптография?
2. Дайте определения следующих понятий: криптограмма, криптоалгоритм, криптосистема.
3. В чем состоит коренное различие симметричных и асимметричных криптосистем?
4. Охарактеризуйте четыре основных режима работы блочного алгоритма.
5. Расскажите о способах комбинирования блочных алгоритмов для получения алгоритмов с более длинным ключом, сравните их между собой.
6. Каковы основные характеристики и режимы работы отечественного стандарта шифрования данных?
7. Сформулируйте концепцию криптосистемы с открытым ключом.
8. Дайте определение однонаправленной функции. Приведите примеры однонаправленных функций.
9. Каковы особенности однонаправленных функций с секретом?
10. На чем основывается надежность криптоалгоритма шифрования RSA?
11. Опишите две основные процедуры, осуществляемые системой электронной цифровой подписи для подтверждения подлинности электронного документа.
12. Опишите отечественный стандарт цифровой подписи, укажите его преимущества по сравнению с алгоритмом цифровой подписи DSA.
13. Каково назначение хэш-функции и каким требованиям должна удовлетворять качественная хэш-функция?
14. Каким образом комбинированный метод шифрования позволяет сочетать достоинства асимметричных и симметричных криптосистем? Опишите протокол реализации комбинированного метода шифрования.
15. Опишите работу алгоритма Диффи — Хэллмана. Укажите достоинства этого алгоритма.
16. Каково назначение инфраструктуры открытых ключей PKI? Опишите функционирование инфраструктуры PKI.

Глава 5
ИДЕНТИФИКАЦИЯ, АУТЕНТИФИКАЦИЯ И УПРАВЛЕНИЕ ДОСТУПОМ

Применение открытых каналов передачи данных создает потенциальные возможности для действий злоумышленников (нарушителей). Поэтому одной из важных задач обеспечения информационной безопасности при взаимодействии пользователей является использование методов и средств, позволяющих одной (проверяющей) стороне убедиться в подлинности другой (проверяемой) стороны. Обычно для решения данной проблемы применяются специальные приемы, дающие возможность проверить подлинность проверяемой стороны.

5.1. Аутентификация, авторизация и администрирование действий пользователей

С каждым зарегистрированным в компьютерной системе субъектом (пользователем или процессом, действующим от имени пользователя) связана некоторая информация, однозначно идентифицирующая его. Это может быть число или строка символов, именующие данный субъект. Эту информацию называют *идентификатором* субъекта. Если пользователь имеет идентификатор, зарегистрированный в сети, он считается легальным (законным) пользователем; остальные пользователи относятся к нелегальным. Прежде чем получить доступ к ресурсам компьютерной системы, пользователь должен пройти процесс первичного взаимодействия с компьютерной системой, который включает идентификацию и аутентификацию.

Идентификация (Identification) — это процедура распознавания пользователя по его идентификатору, присвоенному данному пользователю ранее и занесенному в базу данных в момент его регистрации в качестве легального пользователя системы. Эта функция выполняется в первую очередь, когда пользователь делает попытку войти в сеть. Пользователь сообщает системе по ее запросу свой идентификатор, и система проверяет в своей базе данных его наличие.

Аутентификация (Authentication) — процедура проверки подлинности входящего в систему объекта (пользователя, процесса или устройства), предъявившего свой идентификатор. Эта проверка позволяет дос-

товерно убедиться, что пользователь (процесс или устройство) является именно тем, кем себя объявляет. При проведении аутентификации проверяющая сторона убеждается в подлинности проверяемой стороны, при этом проверяемая сторона тоже активно участвует в процессе обмена информацией. Обычно пользователь подтверждает свою идентификацию, вводя в систему уникальную, не известную другим пользователям информацию о себе (например, пароль или сертификат).

Идентификация и аутентификация являются взаимосвязанными процессами распознавания и проверки подлинности субъектов (пользователей). Именно от них зависит последующее решение системы, можно ли разрешить доступ к ресурсам системы конкретному пользователю или процессу. После идентификации и аутентификации субъекта выполняется его авторизация.

Авторизация (Authorization) — процедура предоставления пользователю (процессу или устройству) определенных прав доступа к ресурсам системы после успешного прохождения им процедуры аутентификации, иными словами, авторизация устанавливает сферу действия пользователя и доступные ему ресурсы. Если система не может надежно отличить авторизованное лицо от неавторизованного, конфиденциальность и целостность информации в этой системе могут быть нарушены. Организации необходимо четко определить свои требования к безопасности, чтобы принимать решения о соответствующих границах авторизации.

С процедурами аутентификации и авторизации тесно связана процедура администрирования действий пользователя. Задачи аутентификации, авторизации и администрирования тесно связаны между собой. Для краткости их взаимосвязанное решение называют решением задач AAA.

Администрирование (Accounting) — это процесс управления доступом пользователей к ресурсам системы.

В настоящее время для решения задач идентификации, аутентификации, авторизации и администрирования используют подсистему управления идентификацией и доступом IAM (Identity and Access Management).

Процесс управления доступом пользователей к ресурсам системы рассматривается в разделе 5.6.

Необходимый уровень аутентификации определяется требованиями безопасности, которые установлены в организации. Общедоступные веб-серверы могут разрешить анонимный или гостевой доступ к информации. Финансовые транзакции могут потребовать строгой аутентификации. Примером слабой формы аутентификации может служить использование IP-адреса для определения пользователя. Подмена (spoofing) IP-адреса может легко разрушить этот механизм аутентификации. Надежная аутентификация является тем ключевым фактором, который гарантирует, что только авторизованные пользователи получат доступ к контролируемой информации.

При защите каналов передачи данных должна выполняться *взаимная аутентификация субъектов*, т. е. взаимное подтверждение подлинности

субъектов, связывающихся между собой по линиям связи. Процедура подтверждения подлинности выполняется обычно в начале сеанса в процессе установления соединения абонентов. Термин «соединение» указывает на логическую связь (потенциально двустороннюю) между двумя субъектами сети. Цель данной процедуры — обеспечить уверенность, что соединение установлено с законным субъектом и вся информация дойдет до места назначения.

Для подтверждения своей подлинности субъект может предъявлять системе разные сущности. В зависимости от предъявляемых субъектом сущностей процессы аутентификации могут быть разделены на следующие категории:

- *на основе знания чего-либо.* Примерами могут служить пароль, персональный идентификационный PIN-код, а также секретные и открытые ключи, знание которых демонстрируется в протоколах типа запрос—ответ;
- *на основе обладания чем-либо.* Обычно это магнитные карты, смарт-карты, сертификаты, USB-ключи или USB-токены (token (англ.) — опознавательный признак, маркер);
- *на основе каких-либо неотъемлемых характеристик.* Эта категория включает методы, базирующиеся на проверке *биометрических характеристик пользователя* (голос, радужная оболочка и сетчатка глаза, отпечатки пальцев, геометрия ладони и др.). В данной категории не используются криптографические методы и средства. Аутентификация на основе биометрических характеристик применяется для контроля доступа в помещения либо к какой-либо технике [7, 49].

Пароль — это то, что знает пользователь и что также знает другой участник взаимодействия. Для взаимной аутентификации участников взаимодействия может быть организован обмен паролями между ними.

Персональный идентификационный номер PIN (Personal Identification Number) является испытанным способом аутентификации держателя пластиковой карты и смарт-карты. Секретное значение PIN-кода должно быть известно только держателю карты.

Динамический (одноразовый) пароль — это пароль, который после однократного применения никогда больше не используется. На практике обычно используется регулярно меняющееся значение, которое базируется на постоянном пароле или ключевой фразе.

Система запрос—ответ — одна из сторон инициирует аутентификацию с помощью посылки другой стороне уникального и непредсказуемого значения «запрос», а другая сторона посылает ответ, вычисленный с помощью «запроса» и секрета. Так как обе стороны владеют одним секретом, то первая сторона может проверить правильность ответа второй стороны.

Сертификаты и цифровые подписи — если для аутентификации используются сертификаты, то требуется применение цифровых подписей на этих сертификатах. Сертификаты выдаются ответственным лицом в организации пользователя, сервером сертификатов или внешней дове-

ренной организацией. В рамках Интернета появился ряд коммерческих инфраструктур управления открытыми ключами PKI для распространения сертификатов открытых ключей. Пользователи могут получить сертификаты различных уровней.

Процессы аутентификации можно также классифицировать по уровню обеспечиваемой безопасности [7, 49]. В соответствии с данным подходом процессы аутентификации разделяются на следующие типы:

- простая аутентификация, использующая пароли;
- строгая аутентификация на основе использования многофакторных проверок и криптографических методов;
- биометрическая аутентификация пользователей.

С точки зрения безопасности каждый из перечисленных типов способствует решению своих специфических задач, поэтому процессы и протоколы аутентификации активно используются на практике.

Основными атаками на протоколы аутентификации являются:

- *маскарад (Impersonation).* Пользователь пытается выдать себя за другого с целью получения полномочий и возможности действий от лица другого пользователя;
- *подмена стороны аутентификационного обмена (Interleaving attack).* Злоумышленник в ходе данной атаки участвует в процессе аутентификационного обмена между двумя сторонами с целью модификации проходящего через него трафика;
- *повторная передача (Replay attack).* Заключается в повторной передаче аутентификационных данных каким-либо пользователем;
- *принудительная задержка (Forced delay).* Злоумышленник перехватывает некоторую информацию и передает ее спустя некоторое время;
- *атака с выборкой текста (Chosen-text attack).* Злоумышленник перехватывает аутентификационный трафик и пытается получить информацию о долговременных криптографических ключах.

Для предотвращения таких атак при построении протоколов аутентификации применяются следующие приемы:

- использование механизмов типа запрос—ответ, меток времени, случайных чисел, идентификаторов, цифровых подписей;
- привязка результата аутентификации к последующим действиям пользователей в рамках системы. Примером подобного подхода может служить осуществление в процессе аутентификации обмена секретными сеансовыми ключами, которые применяются при дальнейшем взаимодействии пользователей;
- периодическое выполнение процедур аутентификации в рамках уже установленного сеанса связи и т. п.

Механизм запроса—ответа состоит в следующем. Если пользователь A хочет быть уверенным, что сообщения, получаемые им от пользователя B, не являются ложными, он включает в посылаемое для B сообщение непредсказуемый элемент — запрос X (например, некоторое случайное число). При ответе пользователь B должен выполнить над этим элементом некоторую операцию (например, вычислить некоторую

функцию $f(X)$). Это невозможно осуществить заранее, так как пользователю B неизвестно, какое случайное число X придет в запросе. Получив ответ с результатом действий B, пользователь A может быть уверен, что B — подлинный. Недостаток этого метода — возможность установления закономерности между запросом и ответом.

Механизм отметки времени подразумевает регистрацию времени для каждого сообщения. В этом случае каждый пользователь сети может определить, насколько устарело пришедшее сообщение, и решить не принимать его, поскольку оно может быть ложным.

В обоих случаях для защиты механизма контроля следует применять шифрование, чтобы быть уверенным, что ответ послан не злоумышленником.

При использовании отметок времени возникает проблема *допустимого временного интервала задержки* для подтверждения подлинности сеанса. Ведь сообщение с «временным штемпелем» в принципе не может быть передано мгновенно. Кроме того, компьютерные часы получателя и отправителя не могут быть абсолютно синхронизированы.

При сравнении и выборе протоколов аутентификации необходимо учитывать следующие характеристики:

- наличие *взаимной аутентификации*. Это свойство отражает необходимость обоюдной аутентификации между сторонами аутентификационного обмена;
- *вычислительная эффективность*. Количество операций, необходимых для выполнения протокола;
- *коммуникационная эффективность*. Данное свойство отражает количество сообщений и их длину, необходимую для осуществления аутентификации;
- *наличие третьей стороны*. Примером третьей стороны может служить доверенный сервер распределения симметричных ключей или сервер, реализующий дерево сертификатов для распределения открытых ключей;
- *гарантии безопасности*. Примером может служить применение шифрования и цифровой подписи [7, 49].

5.2. Методы аутентификации, использующие пароли

Одной из распространенных схем аутентификации является *простая аутентификация*, которая основана на применении традиционных многоразовых паролей с одновременным согласованием средств его использования и обработки. Пока в некоторых защищенных виртуальных сетях VPN доступ клиента к серверу разрешается по паролю. Однако все чаще применяются более эффективные средства аутентификации, например системы аутентификации на основе смарт-карт, USB-токенов, цифровых сертификатов, программные и аппаратные системы аутентификации на основе одноразовых паролей.

5.2.1. Аутентификация на основе многоразовых паролей

В современных операционных системах предусматривается централизованная служба аутентификации, которая выполняется одним из серверов сети и использует для своей работы базу данных. В этой базе данных хранятся учетные данные о пользователях сети. В эти учетные данные наряду с другой информацией включены идентификатор (login) и пароль (password) пользователя.

Процедуру простой аутентификации пользователя в сети можно представить следующим образом. При попытке логического входа пользователя в сеть он набирает на клавиатуре своего компьютера свои идентификатор и пароль. Эти данные поступают для обработки на сервер аутентификации. В базе данных учетных записей пользователей, хранящейся на сервере аутентификации, по идентификатору пользователя находится соответствующая запись, из нее извлекается эталонное значение пароля и сравнивается с тем паролем, который ввел пользователь. Если введенная пользователем пара login/password совпала с эталонной, то аутентификация прошла успешно, пользователь получает легальный статус и те права и ресурсы сети, которые определены для его статуса системой авторизации.

В схеме простой аутентификации передача пароля и идентификатора пользователя может производиться следующими способами [7]:

- в незашифрованном виде: например, согласно протоколу парольной аутентификации PAP (Password Authentication Protocol) пароли передаются по линии связи в открытой незащищенной форме;
- в защищенном виде: все передаваемые данные (идентификатор и пароль пользователя, случайное число и метки времени) защищены посредством шифрования или однонаправленной функции.

Схема простой аутентификации с использованием пароля показана на рис. 5.1.

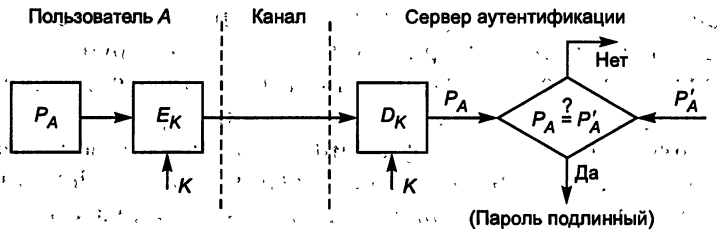


Рис. 5.1. Простая аутентификация с использованием пароля

Очевидно, что вариант аутентификации с передачей пароля пользователя в незашифрованном виде не гарантирует даже минимального уровня безопасности, так как пароль подвержен многочисленным атакам и легко компрометируется. Чтобы защитить пароль, его нужно зашифровать перед пересылкой по незащищенному каналу. Для этого в схему включены средства шифрования E_K и расшифрования D_K, управляемые разделяемым секретным ключом K. Проверка подлинности

пользователя основана на сравнении присланного пользователем пароля P_A и исходного значения P'_A, хранящегося в сервере аутентификации. Если значения P_A и P'_A совпадают, то пароль P_A считается подлинным, а пользователь A — законным.

Схемы организации простой аутентификации отличаются не только методами передачи паролей, но и видами их хранения и проверки. Наиболее распространенным способом является хранение паролей пользователей в открытом виде в системных файлах, причем на эти файлы устанавливаются атрибуты защиты от чтения и записи (например, при помощи описания соответствующих привилегий в списках контроля доступа операционной системы). Система сопоставляет введенный пользователем пароль с хранящейся в файле паролей записью. При этом способе не используются криптографические механизмы, такие как шифрование или однонаправленные функции. Очевидным недостатком данного способа является возможность получения злоумышленником в системе привилегий администратора, включая права доступа к системным файлам и, в частности, к файлу паролей.

Для обеспечения надежной защиты операционной системы пароль каждого пользователя должен быть известен только этому пользователю, и никому другому, в том числе и администраторам системы. На первый взгляд то, что администратор знает пароль некоторого пользователя, не отражается негативно на безопасности системы, поскольку администратор, войдя в систему от имени обычного пользователя, получает права, меньшие, чем те, которые он получит, зайдя в систему от своего имени. Однако, входя в систему от имени другого пользователя, администратор получает возможность обходить систему аудита, а также совершать действия, компрометирующие этого пользователя, что недопустимо в защищенной системе. Таким образом, пароли пользователей не должны храниться в операционной системе в открытом виде.

С точки зрения безопасности предпочтительным является метод передачи и хранения паролей с использованием односторонних функций. Обычно для шифрования паролей в списке пользователей используют одну из известных криптографически стойких хэш-функций. В списке пользователей хранится не сам пароль, а *образ пароля,* являющийся результатом применения к паролю хэш-функции.

Однонаправленность хэш-функции не позволяет восстановить пароль по образу пароля, но позволяет, вычислив хэш-функцию, получить образ введенного пользователем пароля и таким образом проверить правильность введенного пароля. В простейшем случае в качестве хэш-функции используется результат шифрования некоторой константы на пароле.

Например, односторонняя функция $h(\cdot)$ может быть определена следующим образом:

$$h(P) = E_P(ID),$$

где P — пароль пользователя;

ID — идентификатор пользователя;

E_P — процедура шифрования, выполняемая с использованием пароля P в качестве ключа.

Такие функции удобны, если длина пароля и ключа одинакова. В этом случае проверка подлинности пользователя A с помощью пароля P_A состоит из пересылки серверу аутентификации отображения $h(P_A)$ и сравнения его с предварительно вычисленным и хранимым в базе данных сервера аутентификации эквивалентом $h'(P_A)$ — рис. 5.2. Если отображения $h(P_A)$ и $h'(P_A)$ равны, то считается, что пользователь успешно прошел аутентификацию.

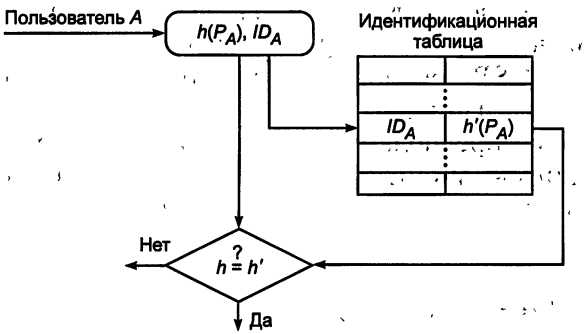


Рис. 5.2. Использование односторонней функции для проверки пароля

Системы простой аутентификации на основе многоразовых паролей имеют пониженную стойкость, поскольку в них выбор аутентифицирующей информации происходит из относительно небольшого множества слов. Срок действия многоразового пароля должен быть определен в политике безопасности организации, и такие пароли должны регулярно изменяться. Выбирать пароли нужно так, чтобы они были трудны для угадывания и не присутствовали в словаре.

Схемы аутентификации, основанные на многоразовых паролях, не обладают достаточной безопасностью. Такие пароли можно перехватить, разгадать, подсмотреть или просто украсть.

5.2.2. Аутентификация на основе одноразовых паролей

Как уже отмечалось, схемы аутентификации, основанные на традиционных многоразовых паролях, не обладают достаточной безопасностью. Более надежными являются процедуры аутентификации на основе одноразовых паролей OTP (One Time Password).

Суть схемы одноразовых паролей — использование различных паролей при каждом новом запросе на предоставление доступа. Одноразовый динамический пароль действителен только для одного входа в систему, и затем его действие истекает. Даже если кто-то перехватил его, пароль окажется бесполезным. Динамический механизм задания пароля является одним из лучших способов защитить процесс аутентификации от угроз извне.

Одноразовые пароли генерируются с помощью OTP-токена. Для этого используется секретный ключ пользователя, размещенный как внутри OTP-токена, так и на сервере аутентификации.

Для того чтобы получить доступ к необходимым ресурсам, пользователь должен ввести пароль, созданный с помощью OTP-токена. Этот пароль сравнивается со значением, сгенерированным на сервере аутентификации, после чего выносится решение о предоставлении доступа. Преимуществом такого подхода является то, что пользователю не требуется соединять токен с компьютером (в отличие от вышеперечисленных типов идентификаторов).

Однако количество приложений ИТ-безопасности, которые поддерживают возможность работы с OTP-токенами, намного меньше, чем для смарт-карт и USB-токенов. Недостатком OTP-токенов является ограниченное время жизни этих устройств (три-четыре года), так как автономность работы предполагает использование батарейки.

Обычно системы аутентификации с одноразовыми паролями используются для проверки удаленных пользователей (см. главу 12).

5.3. Строгая аутентификация

Идея строгой аутентификации заключается в следующем. Проверяемая (доказывающая) сторона доказывает свою подлинность проверяющей стороне, демонстрируя знание некоторого секрета [49, 63]. Этот секрет может быть предварительно распределен безопасным способом между сторонами аутентификационного обмена.

5.3.1. Основные понятия

В соответствии с рекомендациями стандарта X.509 различают процедуры строгой аутентификации следующих типов:

- односторонняя аутентификация;
- двусторонняя аутентификация;
- трехсторонняя аутентификация.

Односторонняя аутентификация предусматривает обмен информацией только в одном направлении. Данный тип аутентификации позволяет:

- подтвердить подлинность только одной стороны информационного обмена;
- обнаружить нарушение целостности передаваемой информации;
- обнаружить проведение атаки типа «повтор передачи»;
- гарантировать, что передаваемыми аутентификационными данными может воспользоваться только проверяющая сторона.

Двусторонняя аутентификация по сравнению с односторонней содержит дополнительный ответ проверяющей стороны доказывающей стороне, который должен убедить ее, что связь устанавливается именно

с той стороной, которой были предназначены аутентификационные данные.

Трехсторонняя аутентификация содержит дополнительную передачу данных от доказывающей стороны проверяющей.

Следует отметить, что данная классификация достаточно условна. Отмеченные особенности носят в большей степени теоретический характер. На практике набор используемых приемов и средств зависит непосредственно от конкретных условий реализации процесса аутентификации.

Как уже отмечалось, процессы строгой аутентификации могут быть реализованы на основе многофакторных проверок и использования криптографических методов.

5.3.2. Двухфакторная аутентификация

Строгая аутентификация может быть реализована на основе двух- или трехфакторного процесса проверки, по результатам которого пользователю может быть предоставлен доступ к запрашиваемым ресурсам.

В первом случае пользователь должен доказать, что он знает пароль или PIN-код и имеет определенный персональный идентификатор (смарт-карту или USB-ключ). Во втором случае пользователь предъявляет еще один тип идентификационных данных, например биометрические данные. На практике более широкое применение находит двухфакторная аутентификация.

Применение средств многофакторной аутентификации снижает роль паролей, и в этом проявляется еще одно преимущество строгой аппаратной аутентификации, так как, по некоторым оценкам, пользователям приходится помнить до 15 различных паролей для доступа к учетным записям. Из-за информационной перегруженности сотрудники, чтобы не забыть пароли, записывают их на бумаге, что снижает уровень безопасности из-за риска компрометации пароля. Использование усиленной, или двухфакторной, аутентификации позволяет не только снизить риски ИТ-безопасности, но и оптимизировать внутренние процессы компании вследствие уменьшения прямых финансовых потерь.

Использование для двухфакторной аутентификации пользователей внешних носителей информации (смарт-карт и USB-токенов) позволяет заметно повысить защищенность системы. В отличие от паролей, владелец быстро узнает о краже внешнего носителя информации и может сразу принять необходимые меры для предотвращения ее негативных последствий.

Аутентификацию на основе смарт-карт и USB-токенов сложнее обойти, так как используется уникальный физический объект, которым должен обладать человек, чтобы войти в систему. Двухфакторная аутентификация на основе смарт-карт и USB-токенов намного надежнее аутентификации с применением многоразовых паролей.

В отличие от простой аутентификации, когда пользователю предоставляется доступ к системе после введения своих имени и пароля, двухфакторная аутентификация имеет другой порядок: взамен пароля пользователь должен предъявить физический носитель — смарт-карту или токен, содержащий сертификат и секретный ключ пользователя. При этом пользователь должен предъявить не только данный носитель секретного ключа, но и ввести PIN-код доступа к носителю, причем ни секретный ключ, ни PIN-код ни в каком виде по корпоративной сети не передаются. Отсутствие передачи секретного ключа и PIN-кода через сеть значительно повышает безопасность процесса аутентификации.

Применение смарт-карт

Смарт-карты — это интеллектуальные пластиковые карты стандартного размера кредитной карты, которые помимо энергонезависимой памяти содержат микропроцессор, способный выполнять криптографические преобразования информации.

По способу обмена данными с устройством ввода-вывода смарт-карты подразделяются на контактные и бесконтактные.

Контактный способ обмена данными подразумевает непосредственное соприкосновение контактов контактной смарт-карты с устройством ввода-вывода.

Бесконтактный (дистанционный) способ обмена данными не требует четкого позиционирования бесконтактной смарт-карты и устройства ввода-вывода. Чтение или запись данных происходит при поднесении бесконтактной смарт-карты на определенное расстояние к устройству ввода-вывода.

Основным компонентом контактных и бесконтактных смарт-карт являются одна или более встроенных интегральных микросхем (чипов), которые могут представлять собой микросхемы памяти, микросхемы с жесткой логикой и микропроцессоры (процессоры). В настоящее время наибольшей функциональностью и степенью защищенности обладают смарт-карты с микропроцессором.

Основу внутренней структуры микропроцессорной смарт-карты составляет чип, в состав которого входят центральный процессор, специализированный криптографический процессор (опционально), оперативная память RAM, постоянная память ROM, электрически перепрограммируемая постоянная память только для чтения EEPROM, датчик случайных чисел, таймеры, последовательный коммуникационный порт (рис. 5.3).

Оперативная память RAM используется для временного хранения данных, например результатов вычислений, произведенных процессором. Ее емкость составляет несколько килобайтов. В постоянной памяти ROM хранятся команды, исполняемые процессором, и другие неизменяемые данные. Информация в ROM записывается при производстве карты. Емкость памяти может составлять десятки килобайтов.

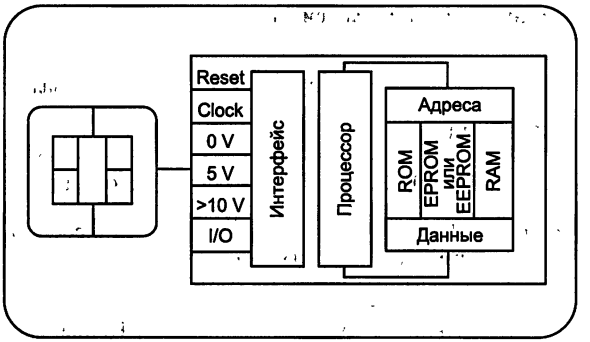


Рис. 5.3. Структура контактной микропроцессорной смарт-карты

В смарт-картах используется два типа памяти PROM: однократно программируемая память EPROM и более распространенная многократно программируемая память EEPROM. В ней хранятся пользовательские данные, которые могут считываться, записываться и модифицироваться, и конфиденциальные данные (например, криптографические ключи), недоступные для прикладных программ. Емкость памяти составляет десятки и сотни килобайт.

Центральный процессор смарт-карты (обычно это RISC-процессор) обеспечивает реализацию разнообразных процедур обработки данных, контроль доступа к памяти и управление ходом выполнения вычислительного процесса.

На специализированный процессор возлагается реализация различных процедур, необходимых для повышения защищенности СИА, в том числе:

- генерация криптографических ключей;
- реализация криптографических алгоритмов (ГОСТ 28147—89, DES, 3-DES, RSA, SHA-1);
- выполнение операций с электронной цифровой подписью (генерация и проверка);
- выполнение операций с PIN-кодом и др.

В постоянной памяти хранится исполняемый код процессора, оперативная память используется в качестве рабочей, EEPROM необходима для хранения изменяемых данных владельца карты.

В отличие от контактных смарт-карт, бесконтактные смарт-карты на базе стандарта MIFARE Standard дополнительно имеют в своем составе радиочастотный модуль со встроенной антенной, необходимой для связи со считывателем и питания микросхемы.

Бесконтактные смарт-карты функционируют на частоте 13,56 МГц и разделяются на два класса, которые базируются на международных стандартах ISO/IEC 14443 и ISO/IEC 15693.

В табл. 5.1 представлены основные характеристики бесконтактных смарт-карт.

Для использования смарт-карт в компьютерных системах необходимо считывающее устройство (или считыватель) смарт-карт. Устройства

Таблица 5.1. **Характеристики бесконтактных смарт-карт**

Характеристика	Смарт-карта стандарт ISO/IEC 14443	Смарт-карта стандарт ISO/IEC 15693
Частота радиоканала, МГц	13,56	13,56
Дистанция чтения	До 10 см	До 1 м
Встроенные типы чипов	Микросхема памяти, микросхема с «жесткой» логикой, процессор	Микросхема памяти, микросхема с «жесткой» логикой
Функции памяти	Чтение/запись	Чтение/запись
Емкость памяти	64 байт — 64 Кб	256 байт — 2 Кб
Алгоритмы шифрования и аутентификации	Технология MIFARE, DES, 3-DES, AES, RSA, ECC	DES, 3-DES
Механизм антиколлизии	Есть	Есть

чтения смарт-карт могут подключаться к компьютеру посредством последовательного порта, слота PCMCIA или USB.

Смарт-карты осуществляют хранение сертификатов пользователей и ключевого материала в самом устройстве, поэтому секретный ключ пользователя не попадает во враждебную внешнюю среду. Для проведения успешной аутентификации требуется вставить смарт-карту в считывающее устройство и ввести пароль (PIN-код). Операционная система считывает идентификатор пользователя и соответствующий ему ключ.

Для хранения и использования закрытого ключа используются разные подходы. Наиболее простой из них — использование устройства аутентификации в качестве защищенного носителя аутентификационной информации: при необходимости карта экспортирует закрытый ключ и криптографические операции осуществляются на рабочей станции. Этот подход является не самым совершенным с точки зрения безопасности, но зато он относительно легко реализуем и предъявляет невысокие требования к устройству аутентификации.

Два других подхода более безопасны, поскольку предполагают выполнение устройством аутентификации криптографических операций.

При первом подходе пользователь генерирует ключи на рабочей станции и сохраняет их в памяти устройства. При втором подходе пользователь генерирует ключи при помощи устройства. В обоих случаях, после того как закрытый ключ сохранен, его нельзя извлечь из устройства и получить любым другим способом.

Генерация ключевой пары вне устройства. В этом случае пользователь может сделать резервную копию закрытого ключа. Если устройство выйдет из строя, будет потеряно, повреждено или уничтожено, пользователь сможет сохранить тот же закрытый ключ в памяти нового устройства. Это необходимо, если пользователю требуется расшифровать какие-либо данные или сообщения, зашифрованные с помощью соответствующего открытого ключа. Однако при этом закрытый ключ поль-

зователя подвергается риску быть похищенным, что означает его компрометацию.

Генерация ключевой пары с помощью устройства. При этом закрытый ключ не появляется в открытом виде, и нет риска его похищения. Единственный способ использования закрытого ключа — это обладание устройством аутентификации. Являясь наиболее безопасным, это решение выдвигает высокие требования к возможностям самого устройства: оно должно обладать функциональностью генерации ключей и осуществления криптографических преобразований. Это решение также предполагает, что закрытый ключ не может быть восстановлен в случае выхода устройства из строя. Подобным образом способны работать микропроцессорные смарт-карты, например Athena ASECard Crypto, Schlumberger Cryptoflex и др.

Следует отметить, что интеллектуальные смарт-карты способны самостоятельно проверять правильность пароля на доступ к ключевой информации, и при аутентификации пользователя с использованием интеллектуальной карты проверку пароля на доступ к карте может производить не операционная система, а сама карта [22]. Интеллектуальная карта может быть запрограммирована на стирание хранимой информации после превышения максимально допустимого количества неправильных попыток ввода пароля, что не позволяет подбирать пароль без частого копирования карты, а это весьма дорого.

Смарт-карты оптимальны для использования в инфраструктуре открытых ключей PKI, так как осуществляют безопасное хранение ключевого материала и сертификатов пользователей в самом устройстве. Достоинством смарт-карты является удобство ее хранения (например, ее можно держать в бумажнике вместе с другими карточками).

Недостатком смарт-карт является низкая мобильность, поскольку для работы с ними требуется считывающее устройство. К недостаткам можно также отнести ограниченный срок эксплуатации из-за неустойчивости смарт-карты к механическим повреждениям и относительно высокую стоимость считывателей смарт-карт.

Применение USB-токенов

USB-токены являются преемниками контактных смарт-карт. Поэтому структуры и функциональность USB-токенов и смарт-карт практически идентичны.

В состав USB-токенов могут входить:

- микропроцессор — управление и обработка данных;
- криптографический процессор — реализация алгоритмов ГОСТ 28147—89, DES, 3-DES, RSA, DSA, MD5, SHA-1 и других криптографических преобразований;
- USB-контроллер — обеспечение интерфейса с USB-портом компьютера;
- оперативная память RAM — хранение изменяемых данных;

- защищенная память EEPROM — хранение ключей шифрования, паролей, сертификатов и других важных данных;
- постоянная память ROM — хранение команд и констант.

Конструктивно USB-ключи выпускаются в виде брелоков (рис. 5.4), которые легко размещаются на связке с обычными ключами. Брелоки выпускаются в цветных корпусах и снабжаются световыми индикаторами работы. Каждый идентификатор имеет прошиваемый при изготовлении собственный уникальный 32/64-разрядный серийный номер.

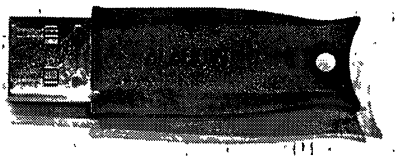


Рис. 5.4. Идентификатор eToken R2

USB-токены со встроенным чипом обладают всеми преимуществами смарт-карт, связанными с безопасным хранением конфиденциальных сведений и осуществлением криптографических операций прямо внутри токена, но лишены их основного недостатка, т. е. не требуют дорогостоящего аппаратного считывателя. USB-токен подключается к USB-порту непосредственно или с помощью соединительного кабеля, поскольку USB является стандартным портом для подключения периферийных устройств.

Процесс двухфакторной аутентификации с использованием USB-токенов проходит в два этапа: пользователь подключает это небольшое устройство в USB-порт компьютера и вводит PIN-код.

Поддержка спецификаций PC/SC позволяет без труда переходить от смарт-карт к USB-ключам и встраивать их как в существующие приложения, так и в новые.

В табл. 5.2 представлены некоторые характеристики USB-токенов.

Таблица 5.2. **Характеристики USB-токенов**

Изделие	Емкость памяти, Кб	Разрядность серийного номера	Алгоритмы шифрования
iKey 20xx	8/32	64	DES (режимы ECB и CBC), 3-DES, RC2, RC4, RC5, MD5, RSA-1024/2048
eToken R2	16/32/64	32	DESX (ключ 120 бит), MD5
eToken PRO	16/32	32	RSA/1024, DES, 3-DES, SHA-1
ePass1000	8/32	64	MD5, MD5-HMAC
ePass2000	16/32	64	RSA, DES, 3-DES, DSA, MD5, SHA-1
ruToken	8/16/32/64/128	32	ГОСТ 28147-89, RSA, DES, 3-DES, RC2, RC4, MD4, MD5, SHA-1

Многофункциональность токенов обеспечивает широкие возможности их применения — от строгой аутентификации и организации безопасного локального или удаленного входа в вычислительную сеть до построения на основе токенов систем юридически важного электронного документооборота, шифрования файлов, организации защищенных каналов передачи данных, управления правами пользователя, осуществления безопасных транзакций и др.

Достоинствами USB-токенов являются малые размеры и удобство хранения, отсутствие аппаратного считывателя, простота подсоединения к USB-порту, высокая мобильность, так как USB-порты имеются на каждой рабочей станции и на любом ноутбуке. Слабым местом USB-токенов является ограниченный ресурс их USB-разъемов. Например, для идентификаторов семейства eToken гарантированное число подключений составляет 5000 раз. К недостаткам можно также отнести относительно высокую стоимость и слабую механическую защищенность брелока.

Особенности использования PIN-кода

Наиболее распространенным методом аутентификации держателя смарт-карты или USB-токена является ввод секретного числа, которое обычно называют *PIN-кодом (Personal Identification Number — персональный идентификационный код)* или иногда CHV (CardHolder Verification). Защита PIN-кода является критичной для безопасности всей системы. Карты могут быть потеряны, украдены или подделаны. В таких случаях единственной контрмерой против несанкционированного доступа остается секретное значение PIN-кода. Вот почему открытая форма PIN должна быть известна только законному держателю карты. Очевидно, значение PIN нужно держать в секрете в течение всего срока действия карты и токена.

Длина PIN-кода должна быть достаточно большой, чтобы минимизировать вероятность определения правильного PIN-кода методом проб и ошибок. С другой стороны, длина PIN-кода должна быть достаточно короткой, чтобы дать возможность держателям карт запомнить его значение. Согласно рекомендации стандарта ISO 9564-1 PIN-код должен содержать от четырех до двенадцати буквенно-цифровых символов. Однако в большинстве случаев ввод нецифровых символов технически невозможен, поскольку доступна только цифровая клавиатура. Поэтому обычно PIN-код представляет собой четырехразрядное число, каждая цифра которого может принимать значение от 0 до 9.

PIN-код вводится с помощью клавиатуры терминала или компьютера и затем отправляется на смарт-карту. Смарт-карта сравнивает полученное значение PIN-кода с эталонным значением, хранимым в карте, и отправляет результат сравнения на терминал. Ввод PIN-кода относится к мерам безопасности, особенно для финансовых транзакций, и, следовательно, требования к клавиатуре часто определяются в этой при-

кладной области. PIN-клавиатуры имеют все признаки модуля безопасности, и они шифруют PIN-код сразу при его вводе. Это обеспечивает надежную защиту против проникновения в клавиатуру для того, чтобы перехватить PIN-код в то время, когда он вводится.

Вероятность угадывания PIN-кода. Простейшей атакой на PIN-код, помимо подглядывания через плечо за вводом его с клавиатуры, является угадывание его значения. Вероятность угадывания зависит от длины угадываемого PIN-кода, от составляющих его символов и от количества разрешенных попыток ввода.

Для оценки риска, связанного с использованием конкретного PIN-кода, могут быть использованы формулы вычисления вероятности угадывания.

Введем обозначения:

x — число возможных комбинаций PIN-кода;

m — число возможных символов на позиции;

n — число позиций в PIN-коде;

P — вероятность угадывания PIN-кода;

i — число попыток угадывания.

Тогда число возможных комбинаций PIN-кода определяется формулой

$$x = m^n.$$

Вероятность угадывания PIN-кода за i попыток определяется формулой $P = i/m^n$.

Если PIN-код состоит из четырех десятичных цифр, т. е. $n = 4$ и $m = 10$, тогда число возможных комбинаций PIN-кода равно $x = m^n = 10^4 = 10\,000$, т. е. злоумышленник, пытающийся угадать значение PIN-кода, оказывается перед проблемой выбора одной из десяти тысяч комбинаций.

Если число разрешенных попыток ввода $i = 3$, тогда вероятность угадывания правильного значения PIN-кода из четырех десятичных цифр за три попытки ввода составляет $P = i/m^n = 3/10^4 = 0{,}00003$, или 0,03 %.

Спецификации PC/SC рекомендуют, чтобы в смарт-картах были установлены ограничения на число неверных попыток ввода PIN-кода. Когда число обнаруженных неверных попыток достигает заданного предела, процесс ввода должен быть заблокирован, препятствуя дальнейшим попыткам аутентификации. Рекомендуется устанавливать допускаемое число неверных попыток в диапазоне от 1 до 255. Метод, используемый для разблокирования процесса ввода, должен быть защищен независимым механизмом аутентификации.

Генерация PIN-кода. Для генерации PIN-кода смарт-карты используются генератор случайных чисел и алгоритм, который преобразует случайное число в PIN-код необходимой длины. Затем можно использовать таблицу известных тривиальных комбинаций, чтобы распознать и отбросить значение PIN-кода, совпадающее с одной из таких комби-

наций. Наконец этот PIN-код записывается в смарт-карту в виде соответствующей криптограммы. Вычисленное значение PIN-кода передается также держателю смарт-карты через защищенный канал.

Главное требование безопасности использования PIN-кода состоит в том, что значение PIN-кода должно запоминаться держателем карты и не должно храниться в любой читаемой форме. Но память людей несовершенна, и часто они забывают значения своих PIN-кодов. Поэтому эмитенты карт должны иметь специальные процедуры для таких случаев. Эмитент может реализовать один из следующих подходов. Первый основан на восстановлении забытого клиентом значения PIN-кода и отправке его обратно владельцу карты. При втором подходе просто генерируется новое значение PIN-кода.

При идентификации клиента по значению PIN-кода и предъявленной карте используются два основных способа проверки PIN-кода: неалгоритмический и алгоритмический [26].

Неалгоритмический способ проверки PIN-кода не требует применения специальных алгоритмов. Проверка PIN-кода осуществляется путем непосредственного сравнения введенного клиентом PIN-кода со значениями, хранимыми в базе данных. Обычно база данных со значениями PIN-кодов клиентов шифруется методом прозрачного шифрования, чтобы повысить ее защищенность, не усложняя процесса сравнения.

Алгоритмический способ проверки PIN-кода заключается в том, что введенный клиентом PIN-код преобразуют по определенному алгоритму с использованием секретного ключа и затем сравнивают со значением PIN-кода, хранящимся в определенной форме на карте. Достоинства этого метода проверки:

- отсутствие копии PIN-кода на главном компьютере исключает его раскрытие обслуживающим персоналом;
- отсутствие передачи PIN-кода между банкоматом или кассиром-автоматом и главным компьютером банка исключает его перехват злоумышленником или навязывание результатов сравнения.

5.3.3. Криптографические протоколы строгой аутентификации

При строгой аутентификации, реализуемой в криптографических протоколах, проверяемая сторона доказывает свою подлинность проверяющей стороне, демонстрируя знание некоторого секрета с использованием криптографических методов и средств.

Существенным является тот факт, что доказывающая сторона демонстрирует только знание секрета, но сам секрет в ходе аутентификационного обмена не раскрывается. Это обеспечивается посредством ответов доказывающей стороны на различные запросы проверяющей стороны. При этом результирующий запрос зависит только от пользовательского

секрета и начального запроса, который обычно представляет произвольно выбранное в начале протокола большое число.

В большинстве случаев строгая аутентификация заключается в том, что каждый пользователь аутентифицируется по признаку владения своим секретным ключом. Иначе говоря, пользователь имеет возможность определить, владеет ли его партнер по связи надлежащим секретным ключом и может ли он использовать этот ключ для подтверждения того, что он действительно является подлинным партнером по информационному обмену.

Необходимо также учитывать, что проведение строгой аутентификации требует обязательного согласования сторонами используемых криптографических алгоритмов и ряда дополнительных параметров [7, 49]. Прежде чем перейти к рассмотрению конкретных вариантов протоколов строгой аутентификации, следует остановиться на назначении и возможностях так называемых одноразовых параметров, используемых в протоколах аутентификации. Эти одноразовые параметры иногда называют *nonces*. По определению, *nonce* — это величина, используемая для одной и той же цели не более одного раза.

Среди используемых на сегодняшний день одноразовых параметров следует выделить случайные числа, метки времени и номера последовательностей.

Одноразовые параметры позволяют избежать повтора передачи, подмены стороны аутентификационного обмена и атаки с выбором открытого текста. При помощи одноразовых параметров можно обеспечить уникальность, однозначность и временные гарантии передаваемых сообщений. Различные типы одноразовых параметров могут употребляться как отдельно, так и дополнять друг друга.

Можно привести следующие примеры применения одноразовых параметров:

- проверка своевременности в протоколах, построенных по принципу запрос—ответ. При такой проверке могут использоваться случайные числа, метки времени с синхронизацией часов или номера последовательностей для конкретной пары (проверяющий, доказывающий);
- обеспечение своевременности или гарантий уникальности. Осуществляется путем непосредственного контроля одноразовых параметров протокола (посредством выбора случайного числа) либо косвенно (путем анализа информации, содержащейся в разделяемом секрете);
- однозначная идентификация сообщения или последовательности сообщений. Осуществляется посредством выработки одноразового значения из монотонно возрастающей последовательности (например, последовательности серийных номеров или меток времени) либо случайных чисел соответствующей длины.

Следует отметить, что одноразовые параметры широко используются и в других вариантах криптографических протоколов (например, в протоколах распределения ключевой информации).

В зависимости от используемых криптографических алгоритмов протоколы строгой аутентификации можно разделить на следующие группы:

- протоколы строгой аутентификации на основе симметричных алгоритмов шифрования;
- протоколы строгой аутентификации на основе однонаправленных ключевых хэш-функций;
- протоколы строгой аутентификации на основе асимметричных алгоритмов шифрования;
- протоколы строгой аутентификации на основе алгоритмов электронной цифровой подписи.

Строгая аутентификация, основанная на симметричных алгоритмах

Для работы протоколов аутентификации, построенных на основе симметричных алгоритмов, необходимо, чтобы проверяющий и доказывающий с самого начала имели один и тот же секретный ключ. Для закрытых систем с небольшим количеством пользователей каждая пара пользователей может заранее разделить его между собой. В больших распределенных системах, применяющих технологию симметричного шифрования, часто используются протоколы аутентификации с участием доверенного сервера, с которым каждая сторона разделяет знание ключа. Такой сервер распределяет сеансовые ключи для каждой пары пользователей всякий раз, когда один из них запрашивает аутентификацию другого. Кажущаяся простота данного подхода является обманчивой, на самом деле разработка протоколов аутентификации этого типа является сложной и с точки зрения безопасности неочевидной.

Протоколы аутентификации с симметричными алгоритмами шифрования. Ниже приводится три примера отдельных протоколов аутентификации, специфицированных в ISO/IEC 9798-2. Эти протоколы предполагают предварительное распределение разделяемых секретных ключей [49, 63].

Рассмотрим следующие варианты аутентификации:

- односторонняя аутентификация с использованием меток времени;
- односторонняя аутентификация с использованием случайных чисел;
- двусторонняя аутентификация.

В каждом из этих случаев пользователь доказывает свою подлинность, демонстрируя знание секретного ключа, так как производит расшифрование запросов с помощью этого секретного ключа.

При использовании в процессе аутентификации симметричного шифрования необходимо также реализовать механизмы обеспечения целостности передаваемых данных на основе общепринятых способов.

Введем следующие обозначения:

r_A — случайное число, сгенерированное участником A;

r_B — случайное число, сгенерированное участником B;

t_A — метка времени, сгенерированная участником A;

E_K — симметричное шифрование на ключе K (ключ K должен быть предварительно распределен между участниками A и B).

1. Односторонняя аутентификация, основанная на метках времени:

$$A \rightarrow B: E_K(t_A, B). \quad (1)$$

После получения и расшифрования данного сообщения участник B убеждается в том, что метка времени t_A действительна и идентификатор B, указанный в сообщении, совпадает с его собственным. Предотвращение повторной передачи данного сообщения основывается на том, что без знания ключа невозможно изменить метку времени t_A и идентификатор B.

2. Односторонняя аутентификация, основанная на использовании случайных чисел:

$$A \leftarrow B: r_B; \quad (1)$$

$$A \rightarrow B: E_K(r_B, B). \quad (2)$$

Участник B отправляет участнику A случайное число r_B. Участник A шифрует сообщение, состоящее из полученного числа r_B и идентификатора B, и отправляет зашифрованное сообщение участнику B. Участник B расшифровывает полученное сообщение и сравнивает случайное число, содержащееся в сообщении, с тем, которое он послал участнику A. Дополнительно он проверяет имя, указанное в сообщении.

3. Двусторонняя аутентификация, использующая случайные значения:

$$A \leftarrow B: r_B; \quad (1)$$

$$A \rightarrow B: E_K(r_A, r_B, B); \quad (2)$$

$$A \leftarrow B: E_K(r_A, r_B). \quad (3)$$

При получении второго сообщения участник B выполняет те же проверки, что и в предыдущем протоколе, и дополнительно расшифровывает случайное число r_A для включения его в третье сообщение для участника A. Третье сообщение, полученное участником A, позволяет ему убедиться на основе проверки значений r_A и r_B, что он имеет дело именно с участником B.

Широко известными представителями протоколов, обеспечивающих аутентификацию пользователей с привлечением в процессе аутентификации третьей стороны, являются протокол распределения секретных ключей Нидхэма и Шредера и протокол Kerberos.

Протоколы, основанные на использовании однонаправленных ключевых хэш-функций

Протоколы, представленные выше, могут быть модифицированы путем замены симметричного шифрования на шифрование с помощью односторонней ключевой хэш-функции [41, 63]. Это бывает необходи-

мо, если алгоритмы блочного шифрования недоступны или не отвечают предъявляемым требованиям (например, в случае экспортных ограничений).

Своеобразие шифрования с помощью односторонней хэш-функции заключается в том, что оно, по существу, является односторонним, т. е. не сопровождается обратным преобразованием — расшифрованием на приемной стороне. Обе стороны (отправитель и получатель) используют одну и ту же процедуру одностороннего шифрования [41].

Односторонняя хэш-функция $h_K(\cdot)$ с параметром-ключом K, примененная к шифруемым данным M, дает в результате хэш-значение m (дайджест), состоящее из фиксированного небольшого числа байтов (рис. 5.5).

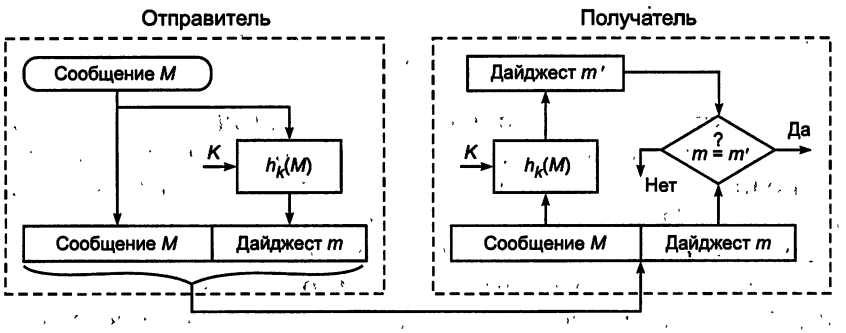


Рис. 5.5. Применение для аутентификации односторонней хэш-функции с параметром-ключом

Дайджест $m = h_K(M)$ передается получателю вместе с исходным сообщением M. Получатель сообщения, зная, какая односторонняя хэш-функция была применена для получения дайджеста, заново вычисляет ее, используя расшифрованное сообщение M. Если значения полученного дайджеста m и вычисленного дайджеста m' совпадают, значит, содержимое сообщения M не было подвергнуто никаким изменениям.

Знание дайджеста не дает возможности восстановить исходное сообщение, но позволяет проверить целостность данных. Дайджест можно рассматривать как своего рода контрольную сумму для исходного сообщения. Однако между дайджестом и обычной контрольной суммой имеется и существенное различие. Контрольную сумму используют как средство проверки целостности передаваемых сообщений по ненадежным линиям связи. Это средство проверки не рассчитано на борьбу со злоумышленниками, которым в такой ситуации ничто не мешает подменить сообщение, добавив к нему новое значение контрольной суммы. Получатель в таком случае не заметит никакой подмены.

В отличие от обычной контрольной суммы, при вычислении дайджеста применяются секретные ключи. В случае если для получения дайджеста используется односторонняя хэш-функция с параметром-ключом K, который известен только отправителю и получателю, любая модификация исходного сообщения будет немедленно обнаружена.

На рис. 5.6 показан другой вариант использования односторонней хэш-функции для проверки целостности данных.

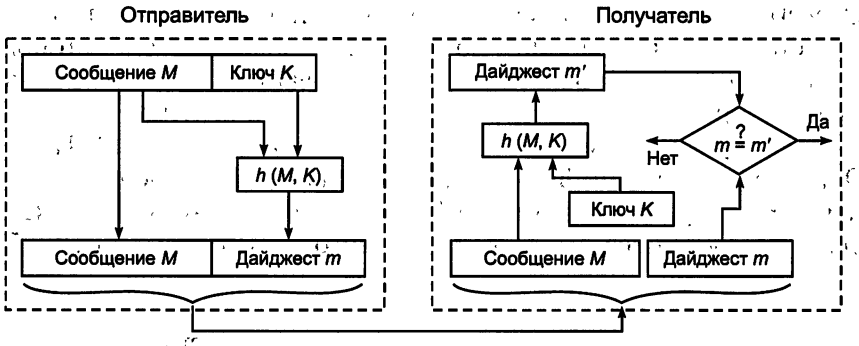


Рис. 5.6. Применение односторонней хэш-функции к сообщению, дополненному секретным ключом K

В этом случае односторонняя хэш-функция $h(\cdot)$ не имеет параметра-ключа, но зато применяется не просто к сообщению M, а к сообщению, дополненному секретным ключом K, т. е. отправитель вычисляет дайджест $m = h(M, K)$. Получатель, извлекая исходное сообщение M, также дополняет его тем же известным ему секретным ключом K, после чего применяет к полученным данным одностороннюю хэш-функцию $h(\cdot)$. Результат вычислений — дайджест m' — сравнивается с полученным по сети дайджестом m.

При использовании для аутентификации односторонних функций шифрования в рассмотренные выше протоколы необходимо внести следующие изменения:

- функция симметричного шифрования E_k заменяется функцией h_k;
- проверяющий вместо установления факта совпадения полей в расшифрованных сообщениях с предполагаемыми значениями вычисляет значение однонаправленной функции и сравнивает его с полученным от другого участника обмена информацией;
- для обеспечения возможности независимого вычисления значения однонаправленной функции получателем сообщения в протоколе 1 метка времени t_A должна передаваться дополнительно в открытом виде, а в сообщении 2 протокола 3 случайное число r_A должно передаваться дополнительно в открытом виде.

Модифицированный вариант протокола 3 с учетом сформулированных изменений имеет следующую структуру:

$$A \leftarrow B: r_B; \quad (1)$$

$$A \rightarrow B: r_A, h_K(r_A, r_B, B); \quad (2)$$

$$A \leftarrow B: h_K(r_A, r_B, A). \quad (3)$$

Заметим, что в третье сообщение протокола включено поле A. Результирующий протокол обеспечивает взаимную аутентификацию и известен как протокол SKID 3 [49, 63].

Строгая аутентификация, основанная на асимметричных алгоритмах

В протоколах строгой аутентификации могут быть использованы асимметричные алгоритмы с открытыми ключами. В этом случае доказывающий может продемонстрировать знание секретного ключа одним из следующих способов:

- расшифровать запрос, зашифрованный на открытом ключе;
- поставить свою цифровую подпись на запросе [49, 63].

Пара ключей, необходимая для аутентификации, не должна использоваться для других целей (например, для шифрования) по соображениям безопасности. Следует также предостеречь потенциальных пользователей о том, что выбранная система с открытым ключом должна быть устойчивой к атакам с выборкой шифрованного текста даже в том случае, если нарушитель пытается получить критичную информацию, выдав себя за проверяющего и действуя от его имени.

Аутентификация с использованием асимметричных алгоритмов шифрования

В качестве примера протокола, построенного на использовании асимметричного алгоритма шифрования, можно привести следующий протокол аутентификации:

$$A \leftarrow B: h(r), B, P_A(r, B); \quad (1)$$

$$A \rightarrow B: r. \quad (2)$$

Участник B выбирает случайным образом r и вычисляет значение $x = h(r)$ (значение x демонстрирует знание r без раскрытия самого значения r), далее он вычисляет значение $e = P_A(r, B)$. Под P_A подразумевается алгоритм асимметричного шифрования (например, RSA), а под $h(\,)$ — хэш-функция. Участник B отправляет сообщение (1) участнику A. Участник A расшифровывает $e = P_A(r, B)$ и получает значения r' и B', а также вычисляет $x' = h(r')$. После этого производится ряд сравнений, доказывающих, что $x = x'$ и что полученный идентификатор B' действительно указывает на участника B. В случае успешного проведения сравнения участник A посылает r. Получив его, участник B проверяет, то ли это значение, которое он отправил в первом сообщении.

В качестве следующего примера приведем модифицированный протокол Нидхэма и Шредера, основанный на асимметричном шифровании. Рассматривая вариант протокола Нидхэма и Шредера, используемый только для аутентификации, будем подразумевать под P_B алгоритм шифрования открытым ключом участника B. Протокол имеет следующую структуру:

$$A \rightarrow B: P_B(r_1, A); \quad (1)$$

$$A \leftarrow B: P_A(r_2, r_1); \quad (2)$$

$$A \rightarrow B: r_2. \quad (3)$$

Аутентификация, основанная на использовании цифровой подписи

В рекомендациях стандарта X.509 специфицирована схема аутентификации, основанная на использовании цифровой подписи, меток времени и случайных чисел.

Для описания данной схемы аутентификации введем следующие обозначения:

t_A, r_A и r_B — временная метка и случайные числа соответственно;
S_A — подпись, сгенерированная участником A;
S_B — подпись, сгенерированная участником B;
$cert_A$ — сертификат открытого ключа участника A;
$cert_B$ — сертификат открытого ключа участника B.

Если участники имеют аутентичные открытые ключи, полученные друг от друга, тогда можно не пользоваться сертификатами, в противном случае они служат для подтверждения подлинности открытых ключей.

В качестве примеров приведем следующие протоколы аутентификации:

1. Односторонняя аутентификация с применением меток времени:

$$A \rightarrow B: cert_A, t_A, B, S_A(t_A, B). \quad (1)$$

После принятия данного сообщения участник B проверяет правильность метки времени t_A, полученный идентификатор B и, используя открытый ключ из сертификата $cert_A$, корректность цифровой подписи $S_A(t_A, B)$.

2. Односторонняя аутентификация с использованием случайных чисел:

$$A \leftarrow B: r_B; \quad (1)$$

$$A \rightarrow B: cert_A, r_A, B, S_A(r_A, r_B, B). \quad (2)$$

Участник B, получив сообщение от участника A, убеждается, что именно он является адресатом сообщения; используя открытый ключ участника A, взятый из сертификата $cert_A$, участник B проверяет корректность подписи $S_A(r_A, r_B, B)$ под числом r_A, полученным в открытом виде, числом r_B, которое было отослано в первом сообщении, и его идентификатором B. Подписанное случайное число r_A используется для предотвращения атак с выборкой открытого текста.

3. Двусторонняя аутентификация с использованием случайных чисел:

$$A \leftarrow B: r_B; \quad (1)$$

$$A \rightarrow B: cert_A, r_A, B, S_A(r_A, r_B, B); \quad (2)$$

$$A \leftarrow B: cert_B, A, S_B(r_A, r_B, A). \quad (3)$$

В данном протоколе обработка сообщений 1 и 2 выполняется так же, как и в предыдущем протоколе, а сообщение 3 обрабатывается аналогично сообщению 2.

5.4. Биометрическая аутентификация пользователя

Процедуры идентификации и аутентификации пользователя могут базироваться не только на секретной информации, которой обладает пользователь (пароль, персональный идентификатор, секретный ключ и т. п.). Привычные системы аутентификации не всегда удовлетворяют современным требованиям в области информационной безопасности, особенно если речь идет об ответственных приложениях (онлайновые финансовые приложения, доступ к удаленным базам данных и т. п.).

В последнее время все большее распространение получает биометрическая аутентификация пользователя, позволяющая уверенно аутентифицировать потенциального пользователя путем измерения физиологических параметров и характеристик человека, особенностей его поведения. Использование решений, основанных на биометрической технологии, позволяет в ряде случаев улучшить положение дел в области аутентификации.

Для методов аутентификации, основанных на использовании многоразовых паролей, характерен следующий недостаток: многоразовый пароль может быть скомпрометирован множеством способов. Недостатком методов, связанных с использованием токенов, является возможность потери, кражи, дублирования токенов — носителей критической информации. Биометрические методы, использующие для идентификации уникальные характеристики пользователя, свободны от перечисленных недостатков.

Отметим основные достоинства биометрических методов аутентификации пользователя по сравнению с традиционными [7]:

- высокая степень достоверности аутентификации по биометрическим признакам из-за их уникальности;
- неотделимость биометрических признаков от дееспособной личности;
- трудность фальсификации биометрических признаков.

В качестве биометрических признаков, которые активно используются при аутентификации потенциального пользователя, можно выделить следующие:

- отпечатки пальцев;
- геометрическая форма кисти руки;
- форма и размеры лица;
- особенности голоса;
- узор радужной оболочки и сетчатки глаз.

Рассмотрим типичную схему функционирования биометрической подсистемы аутентификации. При регистрации в системе пользователь должен продемонстрировать один или несколько раз свои характерные биометрические признаки. Эти признаки (известные как подлинные) регистрируются системой как контрольный образец законного пользователя. Биометрический образец обрабатывается системой для получения информации в виде ЭИП (эталонного идентификатора пользовате-

ля или эталона для проверки). ЭИП представляет собой числовую последовательность, при этом сам образец невозможно восстановить из эталона.

Эталонный идентификатор пользователя хранится системой в электронной форме и используется для проверки идентичности каждого, кто выдает себя за соответствующего законного пользователя. Снятая в процессе идентификации характеристика пользователя сравнивается с ЭИП. Поскольку эти два значения (полученное при попытке доступа и ЭИП) полностью никогда не совпадают, то для принятия положительного решения о доступе степень совпадения должна превышать определенную настраиваемую пороговую величину. В зависимости от степени совпадения или несовпадения совокупности предъявленных признаков с ЭИП лицо, их предъявившее, признается законным пользователем (при совпадении) или нет (при несовпадении).

С точки зрения потребителя, эффективность биометрической аутентификационной системы характеризуется двумя параметрами:

- коэффициентом ошибочных отказов FRR (False-Reject Rate);
- коэффициентом ошибочных подтверждений FAR (False-Alarm Rate).

Ошибочный отказ возникает тогда, когда система не подтверждает личность законного пользователя (типичные значения FRR составляют порядка одной ошибки на 100). *Ошибочное подтверждение* происходит в случае подтверждения личности незаконного пользователя (типичные значения FAR составляют порядка одной ошибки на 10 000). Коэффициент ошибочных отказов и коэффициент ошибочных подтверждений связаны друг с другом; каждому коэффициенту ошибочных отказов соответствует определенный коэффициент ошибочных подтверждений.

В совершенной биометрической системе оба параметра ошибки должны быть равны нулю. К сожалению, биометрические системы не идеальны, поэтому приходится чем-то пожертвовать. Обычно системные параметры настраивают так, чтобы добиться требуемого коэффициента ошибочных подтверждений, что определяет соответствующий коэффициент ошибочных отказов.

К настоящему времени разработаны и продолжают совершенствоваться технологии аутентификации по отпечаткам пальцев, радужной оболочке глаза, по форме кисти руки и ладони, по форме и размеру лица, по голосу и «клавиатурному почерку».

Наибольшее число биометрических систем в качестве параметра идентификации использует отпечатки пальцев (дактилоскопические системы). Отпечаток пальца считается одним из наиболее устойчивых идентификационных признаков (не изменяется со временем, при повреждении кожного покрова идентичный папиллярный узор полностью восстанавливается, при сканировании не вызывает дискомфорта у пользователя).

Дактилоскопические системы аутентификации. Одной из основных причин широкого распространения таких систем является наличие больших банков данных по отпечаткам пальцев. Основными пользова-

телями подобных систем во всем мире являются полиция, различные государственные и некоторые банковские организации.

В общем случае биометрическая технология распознавания отпечатков пальцев заменяет защиту доступа с использованием пароля. Большинство систем используют отпечаток одного пальца, который пользователь предоставляет системе.

Основными элементами дактилоскопической системы аутентификации являются:

- сканер;
- ПО идентификации, формирующее идентификатор пользователя;
- ПО аутентификации, производящее сравнение отсканированного отпечатка пальца с имеющимися в базе данных «паспортами» пользователей.

Дактилоскопическая система аутентификации работает следующим образом. Сначала производится регистрация пользователя. Как правило, производится несколько вариантов сканирования в разных положениях пальца на сканере. Понятно, что образцы будут немного отличаться и требуется сформировать некоторый обобщенный образец, «паспорт». Результаты запоминаются в базе данных аутентификации. При аутентификации производится сравнение отсканированного отпечатка пальца с «паспортами», хранящимися в базе данных.

Формирование «паспорта», так же как и распознавание предъявляемого образца, — это задачи распознавания образов. Для этого используются различные алгоритмы, являющиеся ноу-хау фирм-производителей подобных устройств.

Сканеры отпечатков пальцев. Многие производители все чаще переходят от дактилоскопического оборудования на базе оптики к продуктам, основанным на интегральных схемах.

Продукты на базе интегральных схем имеют значительно меньшие размеры, чем оптические считыватели, и поэтому их проще реализовать в широком спектре периферийных устройств.

Ряд производителей комбинируют биометрические системы со смарт-картами и картами-ключами. Например, в биометрической идентификационной смарт-карте Authentic реализован следующий подход. Образец отпечатка пальца пользователя запоминается в памяти карты в процессе внесения в списки идентификаторов пользователей, устанавливая соответствие между образцом и личным ключом шифрования. Затем, когда пользователь вводит смарт-карту в считыватель и прикладывает палец к сканеру, ключ удостоверяет его личность. Комбинация биометрических устройств и смарт-карт является удачным решением, повышающим надежность процессов аутентификации и авторизации.

Небольшой размер и невысокая цена датчиков отпечатков пальцев на базе интегральных схем превращает их в идеальный для человека интерфейс для систем защиты. Их можно встраивать в брелок для ключей — и пользователи получают универсальный ключ, который обеспечивает защищенный доступ ко всему, начиная от компьютеров до входных дверей, дверец автомобилей и банкоматов.

Системы аутентификации по форме ладони используют сканеры формы ладони, обычно устанавливаемые на стенах. Следует отметить, что подавляющее большинство пользователей предпочитают системы этого типа.

Устройства считывания формы ладони создают объемное изображение ладони, измеряя длину пальцев, толщину и площадь поверхности ладони. Например, продукты компании Recognition Systems выполняют более 90 измерений, которые преобразуются в девятиразрядный образец для дальнейших сравнений. Этот образец может быть сохранен локально, на индивидуальном сканере ладони либо в централизованной базе данных.

По уровню доходов устройства сканирования формы ладони занимают второе место среди биометрических устройств, однако редко применяются в сетевой среде из-за высокой стоимости и размера. Однако сканеры формы ладони хорошо подходят для вычислительных сред со строгим режимом безопасности и напряженным трафиком, включая серверные комнаты. Они достаточно точны и обладают довольно низким коэффициентом ошибочного отказа FRR, т. е. процентом отклоненных законных пользователей.

Системы аутентификации по лицу и голосу являются наиболее доступными из-за их дешевизны, поскольку большинство современных компьютеров имеют видео- и аудиосредства. Системы данного класса применяются при удаленной идентификации субъекта доступа в телекоммуникационных сетях.

Технология сканирования черт лица подходит для тех приложений, где прочие биометрические технологии непригодны. В этом случае для идентификации и верификации личности используются особенности глаз, носа и губ. Производители устройств распознавания черт лица используют собственные математические алгоритмы для идентификации пользователей.

Исследования, проводимые компанией International Biometric Group, говорят о том, что сотрудники многих организаций не доверяют устройствам распознавания по чертам лица отчасти из-за того, что камера их фотографирует, а затем выводит снимки на экран монитора; при этом многие опасаются, что используемая камера низкого качества. Кроме того, по данным этой компании, сканирование черт лица — единственный метод биометрической аутентификации, который не требует согласия на выполнение проверки (и может осуществляться скрытой камерой), а потому имеет негативный для пользователей подтекст.

Следует отметить, что технологии распознавания черт лица требуют дальнейшего совершенствования. Большая часть алгоритмов распознавания черт лица чувствительна к колебаниям в освещении, вызванным изменением интенсивности солнечного света в течение дня. Изменение положения лица также может повлиять на узнаваемость. Различие в положении в 15 % между запрашиваемым изображением и образцом, который находится в базе данных, напрямую сказывается на эффективности. При различии в 45° распознавание становится неэффективным.

Системы аутентификации по голосу экономически выгодны по тем же причинам, что и системы распознавания по чертам лица. В частности, их можно устанавливать с оборудованием (например, микрофонами), поставляемым в стандартной комплектации со многими ПК.

Системы аутентификации по голосу при записи образца и в процессе последующей идентификации опираются на такие уникальные для каждого человека особенности голоса, как высота, модуляция и частота звука. Эти показатели определяются физическими характеристиками голосового тракта и уникальны для каждого человека. Распознавание голоса уже применяется вместо набора номера в определенных системах Sprint. Такой вид распознавания голоса отличается от распознавания речи. В то время как технология распознавания речи интерпретирует то, что говорит абонент, технология распознавания голоса абонента подтверждает личность говорящего.

Поскольку голос можно просто записать на пленку или другие носители, некоторые производители встраивают в свои продукты операцию запроса отклика. Эта функция предлагает пользователю при входе ответить на предварительно подготовленный и регулярно меняющийся запрос, например такой: «Повторите числа 0, 1, 3».

Оборудование аутентификации по голосу более пригодно для интеграции в приложения телефонии, чем для входа в сеть. Обычно оно позволяет абонентам получить доступ в финансовые или прочие системы посредством телефонной связи.

Технологии распознавания говорящего имеют некоторые ограничения. Различные люди могут говорить похожими голосами, а голос любого человека может меняться со временем в зависимости от самочувствия, эмоционального состояния и возраста. Более того, разница в модификации телефонных аппаратов и качество телефонных соединений могут серьезно усложнить распознавание.

Поскольку голос сам по себе не обеспечивает достаточной точности, распознавание по голосу следует сочетать с другими биометриками, такими как распознавание черт лица или отпечатков пальцев.

Системы аутентификации по узору радужной оболочки и сетчатки глаз могут быть разделены на два класса:

- использующие рисунок радужной оболочки глаза;
- использующие рисунок кровеносных сосудов сетчатки глаза.

Сетчатка человеческого глаза представляет собой уникальный объект для аутентификации. Рисунок кровеносных сосудов глазного дна отличается даже у близнецов. Поскольку вероятность повторения параметров радужной оболочки и сетчатки глаза имеет порядок 10^{-78}, такие системы являются наиболее надежными среди всех биометрических систем. Такие средства идентификации применяются там, где требуется высокий уровень безопасности (например, в режимных зонах военных и оборонных объектов).

Биометрический подход позволяет упростить процесс выяснения, «кто есть кто». При использовании дактилоскопических сканеров и устройств распознавания голоса для входа в сети сотрудники избавля-

ются от необходимости запоминать сложные пароли. Ряд компаний интегрируют биометрические возможности в системы однократной аутентификации SSO (Single Sign-On) масштаба предприятия. Подобная консолидация позволяет сетевым администраторам заменить службы однократной аутентификации паролей биометрическими технологиями.

Одной из первых областей широкого применения биометрической аутентификации личности станут *мобильные системы*. Проблема не сводится только к потерям компьютеров из-за краж; нарушение защиты информации может привести к значительно бо́льшим потерям. Кроме того, ноутбуки часто предоставляют доступ к корпоративной сети через программные соединения (выполняемые с помощью паролей, хранящихся на мобильных компьютерах).

Твердотельные датчики отпечатков пальцев — небольшие, недорогие и низкоэнергоемкие — позволяют решить эти проблемы. С помощью соответствующего программного обеспечения эти устройства дают возможность выполнять аутентификацию для четырех уровней доступа к информации, хранящейся на мобильном компьютере: регистрация, выход из режима сохранения экрана, загрузка и дешифровка файлов.

Биометрическая аутентификация пользователя может играть серьезную роль в *шифровании*, в виде модулей блокировки доступа к секретному ключу, который позволяет воспользоваться этой информацией только истинному владельцу частного ключа. Владелец может затем применять свой секретный ключ для шифрования информации, передаваемой по частным сетям или по Интернету.

Ахиллесовой пятой многих систем шифрования является проблема безопасного хранения самого криптографического секретного ключа. Зачастую доступ к ключу длиной 128 или даже больше разрядов защищен лишь паролем из 6 символов, т. е. 48 разрядов. Отпечатки пальцев обеспечивают намного более высокий уровень защиты, и, в отличие от пароля, их невозможно забыть.

5.5. Управление доступом по схеме однократного входа с авторизацией Single Sign-On

Большинство пользователей информационных средств и систем используют компьютеры для доступа к ряду сервисов, будь это несколько локальных приложений или более сложные приложения, которые включают одну или несколько удаленных систем, к которым машина пользователя подсоединяется через сеть. В целях обеспечения безопасности многие приложения требуют проведения аутентификации пользователя прежде, чем ему дадут доступ к сервисам и данным, предоставляемым приложением.

Конечные пользователи обычно воспринимают такие требования системы безопасности как дополнительную нагрузку, которая заставляет их запоминать многочисленные входные идентификаторы и пароли

и использовать их каждый день по нескольку раз, чтобы иметь возможность выполнять свою обычную работу. Довольно обычна ситуация, когда один пользователь имеет пять и более таких пользовательских учетных записей, все на различных платформах с различными правилами для длины паролей, а также с различной частотой их замены. Пользователь должен либо заучивать их все наизусть, либо записывать их туда, где их могут найти неавторизованные пользователи, подвергая тем самым безопасность серьезному риску.

С увеличением числа требующих запоминания паролей возрастает вероятность того, что эти пароли будут забываться, а это потребует от администраторов дополнительных усилий по восстановлению паролей. Эту проблему часто называют «проблемой многих входов». Данную проблему позволяет решить схема однократного входа с авторизацией SSO (Single Sign-On).

Управление доступом по схеме однократного входа с авторизацией SSO дает возможность пользователям корпоративной сети при их входе в сеть пройти одну аутентификацию, предъявив только один раз пароль (или иной требуемый аутентификатор), и затем без дополнительной аутентификации получить доступ ко всем авторизованным сетевым ресурсам, которые им нужны для выполнения их работы. Такими сетевыми ресурсами могут быть принтеры, приложения, файлы и другие данные, размещаемые по всему предприятию на серверах различных типов, работающих на базе различных операционных систем. Управление доступом по схеме однократного входа SSO позволяет повысить производительность труда пользователей сети, уменьшить стоимость сетевых операций и улучшить сетевую безопасность.

С функционированием схемы SSO непосредственно связаны процессы аутентификации и авторизации. С помощью аутентификации система проверяет подлинность пользователя, в то время как авторизация определяет, что именно разрешается делать пользователю (обычно основываясь на его роли в организации). Большинство подходов SSO централизованно осуществляют аутентификацию пользователя. Авторизацию обычно выполняют на ресурсах целевых объектов, хотя некоторые продвинутые SSO-решения централизованно осуществляют и авторизацию — при этом используются продукты централизованного администрирования безопасности, которые осуществляют администрирование полномочий пользователей.

Схему однократного входа SSO поддерживают такие средства, как протокол LDAP (Lightweight Directory Access Protocol), протокол SSL (Secure Sockets Layer), система Kerberos и инфраструктура управления открытыми ключами PKI, а также средства интеграции сервисов каталогов и безопасности. Эти средства и технологии образуют вместе фундамент для применения схемы однократного входа SSO при обработке данных системами, использующими различные комбинации клиентов, серверов, сервисов и приложений.

Существующие решения схемы однократного входа SSO простираются от простых средств до SSO-сервисов на базе сетевых операцион-

ных систем NOS (Network Operating System), многофункциональных приложений и SSO уровня предприятия [7].

SSO-сервисы, основанные на NOS, дают возможность пользователю входить в такие сетевые операционные системы, как Windows NT/2000/XP/Vista, NetWare или Solaris, и таким образом получать доступ ко многим или ко всем приложениям, работающим на базе этой NOS. Компания «Майкрософт» предоставляет возможности интегрированной, всесторонней и простой в использовании SSO на базе операционной системы Microsoft Windows 2000. Схема однократного входа SSO предоставляется в рамках Windows 2000 при помощи встроенных протоколов Kerberos и SSL, которые могут обеспечить стандартные возможности SSO также в смешанных сетях.

Большие приложения, такие как Lotus Notes/Domino или Netscape Communicator/SuiteSpot, допускают один вход для доступа ко всем их прикладным функциям (почте, базам данных, дискуссионным форумам, справочникам, основанным на сертификатах логинам и др.). Многофункциональные приложения не всегда могут интегрировать возможности своих SSO с возможностями тех NOS, на которых они работают. Эти решения позволяют уменьшить число предъявлений пароля, но решают SSO-проблему только в тех случаях, когда пользователи расходуют практически все свое время на многофункциональное приложение, причем это приложение смыкается с сервисами или базами данных и интегрируется с NOS.

SSO-продукты уровня предприятия, такие как IBM's Global Sign-On, CyberSafe's TrustBroker Security Suite и др., обычно применяют комбинированные подходы, основанные на использовании клиентов и прокси; технологии и стандарты кратной аутентификации, включая ввод ID пользователя и пароля с помощью интерфейса командной строки или сценария, вход с помощью API, вход с использованием идентификационных данных от PKI или от Kerberos. Они могут также интегрироваться с NOS и/или средами многофункциональных приложений; в таких случаях они предоставляют пользователю самую широкую область действий. Однако корпоративные SSO-решения могут быть дорогими и сложными для управления.

Сегодня ряд технологий безопасности — межсетевое экранирование, виртуальные защищенные сети VPN, шифрование файлов, аппаратная реализация операционных систем и др. — могут действовать независимо от решения SSO. Со временем многие из этих технологий будут становиться кандидатами на более тесную интеграцию с SSO-решениями.

5.5.1. Простая система однократного входа Single Sign-On

Самое простое SSO-решение состоит в том, чтобы просто автоматизировать процесс предъявления пароля. Для многих из продуктов SSO информация входа (т. е. имя пользователя и пароль) и любые необходимые записи хранятся на специальном сервере аутентификации. Ис-

пользуя клиентское программное обеспечение, пользователь предъявляет серверу аутентификации пароль, и этот сервер сообщает клиентскому программному обеспечению, к каким ресурсам может получить доступ пользователь (рис. 5.7). Клиентское программное обеспечение представляет пользователю допустимые опции. Когда пользователь выберет ресурс, клиентское программное обеспечение использует мандат входа и сценарии, предоставленные сервером аутентификации, чтобы установить от имени пользователя соединение с соответствующим ресурсом целевого объекта (сервера, хоста, домена или приложения).

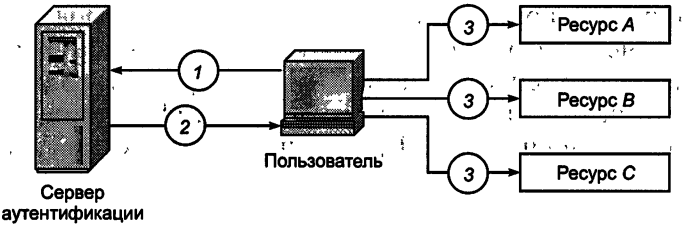


Рис. 5.7. Простое SSO-решение — автоматизация входа

При автоматизации процедуры входа выполняются следующие шаги:

1. Пользователь предъявляет серверу аутентификации пароль, используя специальное клиентское программное обеспечение на своем персональном компьютере.

2. Сервер аутентификации проверяет, к каким ресурсам может получить доступ этот пользователь, и отправляет эту информацию обратно на клиентское SSO-приложение совместно с необходимым мандатом входа и сценариями для соединения с каждым разрешенным ресурсом.

3. Клиентское SSO-приложение представляет пользователю доступные ресурсы и входит от имени пользователя в выбранные приложения.

Автоматизация процедуры входа позволяет получить простую схему SSO, но при этом еще больше децентрализуется администрирование безопасностью. Ряд поставщиков предлагают дополнительные средства централизованного администрирования безопасностью. Эти средства используют агентов в целевых системах и обеспечивают основанное на ролях (role-based) централизованное администрирование учетных записей пользователей и информации об их полномочиях. В некоторых случаях эти средства администрирования полностью отделены от схемы SSO; в других случаях они интегрированы с SSO.

Первоначальной целью SSO было сокращение числа используемых многоразовых паролей для получения пользователями доступа к сетевым ресурсам. При формировании современного решения SSO применяются также такие средства аутентификации пользователя, как токены, цифровые сертификаты PKI, смарт-карты и биометрические устройства. Более совершенный подход к аутентификации обычно ос-

нован на использовании токенов. Наиболее известной системой аутентификации является Kerberos (в качестве механизма аутентификации Kerberos поддерживают IBM, «Майкрософт», CyberSafe и ряд других компаний).

Продвинутые SSO-решения также предоставляют больше контроля над полномочиями пользователя, поддерживаемыми обычно на прикладном уровне. Минимально такие решения включают агентов для общего сервера и сред приложений, которые обеспечивают централизованное, основанное на ролях администрирование полномочий пользователя по нескольким ресурсам. Целевой ресурс доверяет SSO-системе идентифицировать конкретных пользователей и их роли; SSO эффективно доставляет доверенные мандаты к приложению, скрывая от приложения процесс аутентификации. Поэтому продукты SSO могут также поддерживать не-токенные механизмы аутентификации, например основанные на сертификатах PKI (в частности, RSA ClearTrust поддерживает PKI).

5.5.2. Системы однократного входа Web SSO

Разработчики первых веб-сайтов были вынуждены создавать свои собственные SSO-решения и столкнулись с рядом трудностей. Однако вскоре разработчики Web SSO получили помощь в виде cookie со стороны поставщиков веб-браузеров. Компании «Майкрософт» и Novell — два главных поставщика веб-браузеров — очень рано ввели в своих продуктах поддержку cookie. В качестве cookie могут быть использованы зашифрованные данные пользователя (зашифрованный мандат пользователя). Cookie — это часть информации, которую веб-сервер хранит на ПК пользователя с помощью браузера и которую можно использовать при принятии решения о предоставлении пользователю доступа, поэтому cookie стали широко распространенным и популярным механизмом для создания Web SSO. Если имя пользователя хранится в cookie на компьютере пользователя, серверное приложение может проверить, кем является этот пользователь, не предлагая ему предъявлять пароль снова, независимо от того, на какую страницу сайта переходит этот пользователь.

Проблема однократного входа с авторизацией SSO была успешно решена во Всемирной паутине, поскольку не было иного выбора — требование веб-сайтом многократного предъявления пароля является просто недопустимым вариантом. Действительно, коммерческий веб-сайт, который потребует от посетителя сайта предъявить пароль несколько раз за сессию, подвергнет суровому испытанию терпение посетителей и быстро растеряет всех своих потенциальных клиентов. В настоящее время схема однократного входа SSO на веб-сайт является практически обязательным сервисом (рис. 5.8). Следует отметить, что большинство продвинутых корпоративных веб-сайтов извлекают свои данные из серверных баз данных.

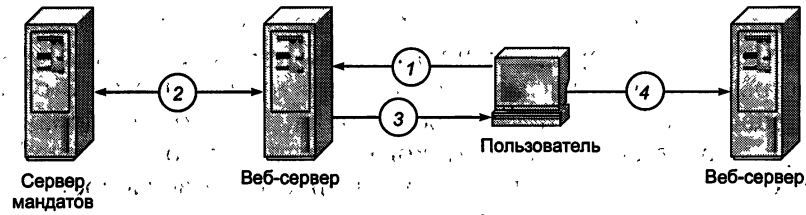


Рис. 5.8. Схема Web SSO, основанная на использовании cookie

В схеме Web SSO, основанной на использовании cookie, при реализации процедуры входа выполняются следующие шаги:

1. (1) Пользователь, применяя специальное клиентское программное обеспечение на своем персональном компьютере, передает на веб-сервер имя пользователя и пароль.

2. Агент веб-сервера извлекает мандат пользователя с сервера мандатов (Credentials Server). Веб-сервер предоставляет пользователю ресурсы в соответствии с его мандатом.

3. Агент веб-сервера сохраняет зашифрованный мандат в качестве cookie на компьютере пользователя.

4. Когда пользователь переходит на другую страницу на веб-сайте, которая может быть на другом веб-сервере, последний просто читает мандат пользователя из его cookie.

Вскоре после своего появления cookie стали подвергаться атакам, но поскольку теперь cookie могут передаваться с помощью шифрованной SSL-сессии, эта проблема практически исключена. Позднее Java обеспечил гибкость программирования на стороне браузера, что образует базу для других SSO-подходов в Сети.

На рис. 5.9 показана схема Web SSO, не использующая cookie.

В схеме Web SSO, не использующей cookie, при реализации процедуры входа выполняются следующие шаги:

1. Пользователь передает на веб-сервер имя пользователя и пароль.

2. Агент на веб-сервере извлекает мандат пользователя с сервера мандатов. Веб-сервер предоставляет пользователю ресурсы в соответствии с его мандатом.

3. Если пользователь пытается получить доступ к защищенным ресурсам на другом веб-сервере...

4. ...агент на этом веб-сервере должен снова запрашивать мандат пользователя на сервере мандатов.

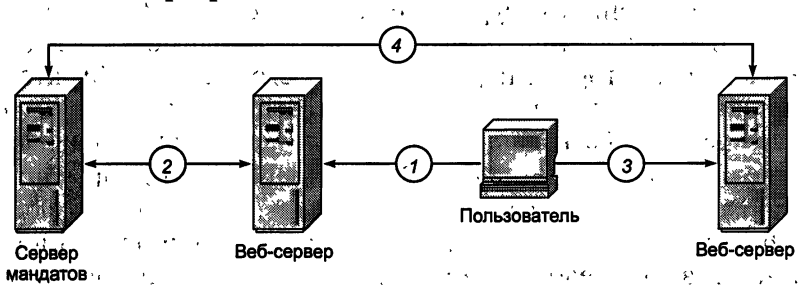


Рис. 5.9. Схема Web SSO, не использующая cookie

Коммерческие решения Web SSO используют ряд подходов. Почти во всех подходах требуется использование агентов, установленных на веб-серверы, которые связываются с отдельным мандатным сервером, чтобы проверить подлинность пользователя. Некоторые варианты также требуют собственного клиентского программного обеспечения. Такой подход может дать более высокий уровень безопасности при использовании технологий аутентификации на основе одноразовых токенов или возможностей PKI.

Сегодня многие организации подсоединены к Интернету, так что, по существу, образована одна большая сеть с разными политиками безопасности, осуществляемыми в разных сегментах этой сети. Безопасность корпоративной сети прежде всего реализуется по периметру между корпоративной сетью и открытым Интернетом. Поэтому при рассмотрении проблемы безопасности корпоративной сети пользователей разделяют на внутренних и внешних. Однако реальное различие между пользователями состоит не в том, внешние они или внутренние, а в том, авторизованы они или нет в данной организации. В рационально организованной компании сотрудники, заказчики, поставщики и бизнес-партнеры имеют доступ только к той информации, которая им нужна для их деятельности согласно предписанным ролям в этой компании.

5.5.3. SSO-продукты уровня предприятия

SSO-продукты уровня предприятия проектируются для больших компаний с гетерогенной распределенной компьютерной средой, состоящей из многих систем и приложений. Схема однократного входа с авторизацией SSO дает возможность пользователям корпоративной сети при их входе в сеть пройти одну аутентификацию, а затем получить доступ к сетевым ресурсам, которые им нужны для выполнения их работы. Такими сетевыми ресурсами могут быть приложения, файлы и другие данные, размещаемые по всему предприятию на серверах различных типов, работающих на базе различных операционных систем.

Характерным представителем SSO-продуктов уровня предприятия является продукт IBM Global Sign-On for Multiplatforms (далее называемый GSO). Продукт GSO представляет собой безопасное, простое в использовании решение, позволяющее пользователю получать доступ к сетевым компьютерным ресурсам, используя однократный вход в систему. GSO освобождает пользователя от необходимости вводить различные идентификаторы и пароли для всех его целевых объектов, которые включают операционные системы, совместно используемые программные средства, базы данных или приложения другого вида [7].

Было бы идеально, если бы GSO мог действовать как универсальный, безопасный, надежный механизм аутентификации для любого целевого объекта. К сожалению, такое решение унифицированной аутентификации создать невозможно, потому что большинство продуктов, которым требуется сервис аутентификации, выполняют процедуру

аутентификации различным образом. Чтобы сделать реальностью такой идеальный подход, поставщики должны модифицировать свои продукты с целью обеспечить выполнение требований общего стандарта X/Open Single Sign-On (XSSO).

Поэтому GSO придерживается реального подхода, основанного на том факте, что продукты поставщиков не поддерживают доверенную внешнюю аутентификацию. Для аутентификации эти продукты чаще всего требуют идентификатор ID и пароль каждого пользователя. GSO осуществляет безопасное хранение пользовательских идентификаторов ID и паролей и обеспечение ими целевых объектов, когда пользователю нужно предъявить пароль при входе. Это освобождает пользователя от необходимости помнить и вводить эти ID и пароли каждый день для каждого целевого объекта.

На рис. 5.10 показана базовая схема ячейки GSO. Ячейка GSO содержит по крайней мере сервер GSO и одну рабочую станцию пользователя, называемую также клиентом GSO. В ячейке GSO может быть более одного сервера GSO и множество клиентов.

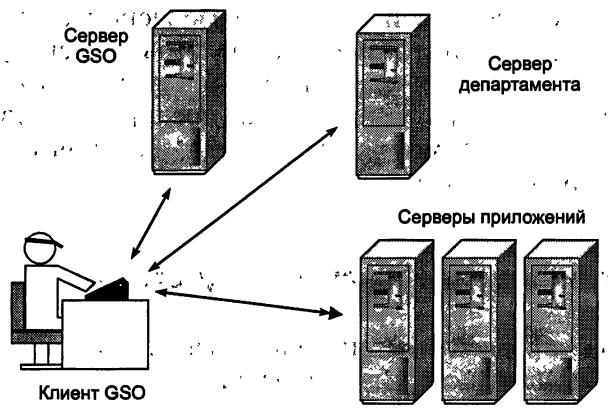


Рис. 5.10. Базовые компоненты GSO

Пользователь взаимодействует со своей рабочей станцией и некоторыми целевыми объектами (приложениями), которые могут выполняться на этой рабочей станции или на каком-либо другом компьютере, например сервере департамента или серверах приложений.

Перед тем как начать работу, пользователь должен войти на свою рабочую станцию. Пользователь предъявляет пароль именно GSO, а не приложению или другим серверам. GSO выполняет аутентификацию, основанную на идентификаторе ID и пароле пользователя (иногда поддерживаемых смарт-картой или считывателем отпечатков пальцев). Сервер GSO включается в процесс аутентификации для того, чтобы проверить пароль пользователя и извлечь его мандат (credential).

Затем GSO будет вводить пользователя в целевые объекты (приложения или серверы), с которыми этот пользователь должен работать. GSO использует для входа пользователя методы, предоставляемые це-

левыми объектами. В большинстве случаев GSO имитирует вход пользователя, передавая целевому объекту ID и пароль пользователя, как будто вводит их сам пользователь. Важное различие, очевидно, состоит в том, что теперь пользователю не нужно запоминать эти идентификаторы ID и пароли, поскольку заботу о них принимает на себя GSO.

GSO является клиент/серверным приложением. В дополнение к серверу GSO существует программа клиента (сегмент программного кода), выполняемая на рабочей станции пользователя, которая взаимодействует с сервером GSO [7].

SSO-продукты уровня предприятия обладают следующими достоинствами:

- допускают использование многих целевых платформ со своими собственными механизмами аутентификации;
- безопасно хранят в базах данных учетную информацию каждого пользователя (такую, как идентификатор ID, пароль и некоторая дополнительная информация) на каждую целевую платформу;
- радикально уменьшается доля забываемых паролей, поскольку пароли пользователей хранятся безопасно и надежно.
- используются методы и средства безопасной аутентификации и коммуникации. Чувствительная пользовательская информация хранится и передается по сети только в зашифрованном виде.

Недостатками SSO-продуктов уровня предприятия является их относительно большая стоимость и высокие требования к квалификации обслуживающего персонала.

5.6. Управление идентификацией и доступом

Подсистема управления идентификацией и доступом IAM (Identity and Access Management) строится на основе:

- средств аутентификации;
- системы централизованного управления учетными записями и правами доступа;
- служб каталогов.

Основные методы и средства аутентификации были подробно рассмотрены в предыдущих разделах данной главы.

Процессы идентификации и аутентификации неразрывно связаны с системой управления доступом к ресурсам системы. В самом деле, если нет возможности точно идентифицировать того, кто работает с системой, то невозможно грамотно распределить уровни доступа к информации. С другой стороны, если нет системы управления доступом, то теряет смысл и сама система аутентификации. Эти системы необходимо планировать и внедрять комплексно, в едином ключе, поскольку ни одна из этих систем не является полнофункциональной без другой.

Процесс управления доступом пользователей включает в себя:

- создание идентификатора субъекта (создание учетной записи пользователя) в системе;

- управление данными субъекта, используемыми для его аутентификации (смена пароля, издание сертификата и т. п.);
- управление правами доступа субъекта к ресурсам системы.

В зависимости от конкретных задач может потребоваться доступ к различным ресурсам:

- к операционным системам;
- к базам данных;
- к сетевым ресурсам;
- к веб-ресурсам.

Система централизованного управления учетными записями и правами доступа пользователей предназначена для повышения безопасности корпоративных приложений и сервисов и снижения затрат на администрирование в разнородных приложениях и операционных системах.

Эта система осуществляет синхронизацию, распространение и централизованное управление правами и учетными записями в гетерогенных информационных системах и приложениях на основе единого, централизованного представления учетных записей.

В общем случае подсистема управления учетными записями состоит из центрального хранилища учетных записей (служба каталогов), политик управления записями, правил распространения учетных записей в целевые системы и механизма согласования учетных записей.

При получении информации от целевых систем о создании/изменении/удалении учетных записей локальными средствами администрирования подсистема выполняет определенные действия в соответствии с заданными политиками.

При создании учетной записи пользователя в центральной системе (кадровая система, служба каталога и т. п.) подсистема управления учетными записями производит автоматическую трансформацию записи в идентификационные записи в целевых системах согласно политикам управления.

Такой подход позволяет реализовать модель ролевого управления пользователями, которые автоматически получают необходимые им права на ресурсы в соответствии с должностными обязанностями, определенными через включение их в соответствующие ролевые группы.

Одной из ключевых задач подсистемы управления учетными записями является автоматическое изменение параметров или удаление учетных записей пользователей, которые уже не работают в компании или ушли в плановый отпуск и не должны иметь доступ к ресурсу.

С ростом числа пользователей информационной системы и количества прикладных систем и сервисов, к которым они должны получать доступ, увеличиваются затраты на администрирование учетных записей пользователей и управление правами доступа к системам и сервисам.

Использование системы централизованного управления учетными записями и правами доступа позволяет автоматизировать процессы, связанные с созданием, администрированием, удалением учетных записей, предоставлением доступа к ресурсам и управлением правами в раз-

народных операционных системах, службах каталогов и приложениях. Благодаря этому снижается нагрузка на ИТ-персонал предприятия.

Использование решений централизованного управления учетными записями и правами доступа позволяет сократить расходы на ведение учетных записей в корпоративных системах, так как создание/изменение/удаление учетных записей проводится один раз в центральной системе и далее эта информация через центральное хранилище передается в целевые системы автоматически (иногда такой подход называется концепцией единой сущности учетной записи).

Архитектура решений для управления учетными записями позволяет иметь одно представление пользователя в различных системах и позволяет избежать повторного ввода идентификационных данных, связанных с этим ошибок и рассогласования учетных записей в корпоративных системах.

Дополнительно решения позволяют установить единые для организации правила в отношении паролей на доступ к системам и уменьшить временные затраты администраторов ИТ-подразделения, связанные со сменой и восстановлением паролей пользователей.

Благодаря решениям централизованного управления учетными записями и правами доступа администраторы безопасности могут быть уверены в том, что установленные политики безопасности в отношении паролей действительно используются и отсутствуют забытые или неучтенные учетные записи в информационной системе организации.

Системы однократной аутентификации SSO предназначены для автоматической аутентификации пользователей в целевых системах и приложениях. Логика работы системы SSO основывается на принципе хранения секретных данных пользователей в центральном хранилище (базе данных, службе каталогов).

Учетные данные системы SSO записываются в центральное хранилище (службу каталога) при первом входе пользователя в поддерживаемое приложение либо могут быть внесены в него администратором системы вручную или в результате интеграции с системой централизованного управления учетными записями и правами доступа. Поэтому системы SSO могут выступать в качестве альтернативы системе централизованного управления учетными записями и правами доступа либо дополнять эту систему.

Вопросы для самоконтроля

1. Дайте определение понятий «идентификация», «аутентификация», «авторизация», «администрирование».
2. Что понимают под решением задач AAA?
3. Какие задачи решает подсистема управления идентификацией и доступом IAM?
4. На какие категории можно разделить процессы аутентификации в зависимости от сущностей, предъявляемых пользователем для подтверждения своей подлинности?

5. Перечислите основные атаки на протоколы аутентификации.
6. Опишите метод аутентификации на основе многоразовых паролей. Каковы его недостатки?
7. Опишите метод аутентификации на основе одноразовых паролей. Каковы его достоинства и недостатки?
8. Сформулируйте принцип строгой аутентификации. Опишите типы процедур строгой аутентификации.
9. Объясните назначение PIN-кода и особенности его использования.
10. Объясните принцип работы двухфакторной аутентификации. Какие внешние носители информации используют для двухфакторной аутентификации пользователей? Каковы достоинства этого метода аутентификации?
11. Опишите функциональность и характеристики смарт-карт и USB-токенов.
12. Опишите методы биометрической аутентификации пользователя.
13. Что означают термины «коэффициент ошибочных отказов» и «коэффициент ошибочных подтверждений»?
14. Объясните принцип управления доступом по схеме однократного входа с авторизацией SSO.

Глава 6
ЗАЩИТА ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА

Системы электронного документооборота играют важную роль в управлении организациями, имеющими разветвленную сеть подразделений, филиалов и представительств. Система электронного документооборота является характерным примером прикладной информационной системы. Чем глубже прикладные информационные системы интегрируются в бизнес организаций, тем сильнее бизнес зависит от надежности этих систем. Внешние и внутренние злоумышленники могут нарушить конфиденциальность, целостность и доступность обрабатываемых в прикладных системах данных. Нарушение нормального функционирования системы электронного документооборота и корпоративной информационной системы в целом может привести к прямым потерям для организации.

6.1. Концепция электронного документооборота

Электронный документооборот — это способ организации работы с документами, при котором основная масса документов организации (предприятия) используется в электронном виде и хранится централизованно.

Система электронного документооборота (СЭД) — компьютерная программа (программное обеспечение, система и т. п.), которая позволяет организовать работу с электронными документами (создание, изменение, поиск), а также взаимодействие между сотрудниками (передачу документов, выдачу заданий, отправку уведомлений и т. п.).

Иногда СЭД называют EDMS (Electronic Document Management Systems) — системой управления электронными документами. Системы электронного документооборота обычно относят к классу прикладных систем управления корпоративными информационными ресурсами ECM (Enterprise Content Management) [103].

Под системой ECM понимают набор технологий, инструментов и методов, используемых для сбора, управления, накопления, хранения и доставки информации (контента) всем потребителям внутри организации. Это понятие несколько шире, чем СЭД. Например, для того чтобы

стать ECM-системой, СЭД должна содержать средства сканирования документов, гарантировать сохранность документов, поддерживать правила хранения документов и т. д.

По сравнению с бумажным документооборотом электронный документооборот имеет ряд преимуществ:

- *сокращение затрат времени руководителей и сотрудников.* Использование СЭД сокращает временные затраты практически на все рутинные операции с документами (создание, поиск, согласование и т. д.). Кроме того, происходит ускорение документооборота и, как следствие, всех процессов в организации;
- *исключение несанкционированного доступа.* В отличие от традиционного «бумажного» документооборота, СЭД обеспечивает доступ к документам строго в соответствии с назначенными правами пользователей, все действия над документом (чтение, изменение, подписание) протоколируются;
- *прозрачность бизнес-процессов.* Система обеспечивает возможность отслеживания этапов выполнения бизнес-процессов, благодаря чему вся деятельность в организации оказывается абсолютно прозрачной для руководства и контролируемой среды;
- *повышение исполнительской дисциплины.* Предоставляя полный контроль всех этапов работ для руководства, СЭД напрямую влияет на исполнительскую дисциплину сотрудников;
- *легкость внедрения инноваций и обучения.* Благодаря системе оповещения, построенной на базе системы СЭД, можно быстро доводить новые правила работы до всех сотрудников. Сокращаются сроки обучения новых сотрудников. Легко меняются маршруты прохождения и шаблоны документов, после чего сотрудники автоматически начинают работать по-новому;
- *развитие корпоративной культуры.* Процесс внедрения электронного документооборота налаживает и поддерживает корпоративную культуру. Возрастает ответственность каждого сотрудника за качественное выполнение выданного ему задания;
- *рост конкурентных преимуществ.* Внедрение СЭД напрямую отражается на конкурентных преимуществах компании перед другими игроками рынка. Повышается скорость и качество обслуживания клиентов за счет ускорения движения информационных потоков и четкого контроля всех процессов.

Системы электронного документооборота функционируют на предприятиях и в учреждениях, работающих в самых разных отраслях и сферах деятельности.

Базовые составляющие СЭД

Рассмотрим базовые составляющие современной системы электронного документооборота, необходимые для обеспечения поддержки работы предприятий с развитыми связями.

К базовым составляющим СЭД относятся следующие подсистемы:

- идентификация и аутентификация пользователей;
- разграничение доступа к объектам;
- автоматизация управления рабочими процессами;
- управление электронными документами;
- регистрация событий в СЭД.

Подсистема идентификации и аутентификации пользователей

Идентификация и аутентификация обычно осуществляются путем набора системного имени и пароля (пара логин—пароль). Эти данные хранятся на сервере в специальной базе данных пользователей, причем в большинстве случаев предъявляется требование хранить их или только пароль в защищенном виде. В качестве механизма защиты может быть использовано шифрование или хэширование.

В последнее время для подтверждения полномочий пользователя используют специальные носители информации (USB-ключи, смарт-карты).

Реализация рассматриваемой подсистемы может отличаться в разных системах электронного документооборота. В частности, эта подсистема может быть выделена в отдельный модуль или включена в исполняемый код клиентских приложений.

Подсистема разграничения доступа к объектам

В любой системе электронного документооборота обязательно должно быть предусмотрено разграничение прав пользователей.

Разграничение прав пользователей внутри системы технически выполняется по-разному: это может быть полностью своя подсистема, созданная разработчиками СЭД, или подсистема безопасности СУБД, которую использует СЭД. Иногда встречаются комбинированные решения, использующие свои разработки и подсистемы СУБД. Такая комбинация предпочтительнее — она позволяет закрыть возможные недостатки подсистем безопасности СУБД.

Подсистема автоматизации управления рабочими процессами

Подсистема автоматизации управления рабочими процессами (WorkFlow) реализует все функции, относящиеся к контролю исполнения: создание поручений исполнителям, задание сроков исполнения для поручений и всего документа, создание подпоручений, назначение контролеров поручений и документов, отслеживание сроков работ над поручениями и документами, рассылку уведомлений о назначении контролерами и исполнителями, а также уведомлений о приближении и истечении сроков работ.

Система управления рабочими процессами тесно интегрирована с почтовой системой, используемой в электронном документообороте. Это может быть своя собственная почтовая система или стандартная электронная почта.

Подсистема управления электронными документами

Эта система обеспечивает создание электронных документов, их перемещение между клиентом и сервером, перемещение между пользователями, поиск, просмотр, организацию процесса редактирования, а также удаления документов. Указанная функциональность может быть реализована в различных программных модулях, ее локализация в рамках одного модуля встречается достаточно редко.

Для реализации перечисленных действий требуется совместная работа как клиента, так и сервера.

Подсистема регистрации событий в СЭД

Протоколирование действий пользователей в системах электронного документооборота является общепринятой функцией. Это необходимо как для обеспечения информационной безопасности, так и для выяснения истории документов. Возможны различные варианты реализации настроек протоколов и их просмотра.

Следует отметить также применение в СЭД подсистем формирования отчетов, разработки отчетных форм и регистрационных карточек, администрирования и хранения документов.

Распределенный электронный документооборот

После успешной автоматизации делопроизводства предприятия возникает задача автоматизации взаимодействия смежных организаций. Примером такого взаимодействия является обмен документами и распоряжениями между центральным офисом холдинга и его филиалами, аналогичные задачи возникают и внутри крупной организации (общение подразделений между собой).

При рассмотрении схемы построения распределенного документооборота наиболее естественным вариантом является схема с единым центральным сервером.

Этот сервер может выполнять различные функции — хранилища контактной информации о серверах предприятий, хранилища информации о пользователях, зарегистрированных на различных серверах, и хранилища документов, введенных в систему всеми участвующими в документообороте предприятиями.

Такая централизованная схема имеет очевидные достоинства, обусловленные простой процедурой установления связи между серверами

и возможностью поиска чужих документов. Однако ее недостатком является нарушение работоспособности всего комплекса в случае выхода из строя центрального компьютера. Кроме того, в этом случае возникает проблема репликации данных между серверами, что само по себе непросто как технически, так и организационно.

Другой вариант архитектуры распределенной СЭД — схема с равноправными серверами предприятий. Этот вариант предполагает, что все участвующие в системе серверы абсолютно равноправны с точки зрения их программного обеспечения, а «выделенность» сервера центрального офиса проявляется в логике работы пользователей, в бизнес-логике, а не в технической реализации. К преимуществам такой схемы можно отнести жизнеспособность системы при сбоях отдельных серверных компьютеров, простоту настройки системы в целом, отсутствие репликации данных. Конечно, простота настройки, заключающаяся в отсутствии необходимости обслуживания центрального сервера, приводит к усложнению настройки каждого сервера системы. Это выражается в том, что для каждой пары взаимодействующих серверов потребуется задать некоторый набор настроек, позволяющий передавать данные между ними — адреса для связи (IP-, электронной почты), список пользователей, правила приема документов и ряд других.

В любой СЭД работа с документами регламентируется с помощью системы разграничения прав доступа к объектам. В данном случае предполагается, что права доступа будут задаваться сотрудникам внешних предприятий по той же схеме, что и для своих коллег.

Принципиально возможна схема организации работы, направленная на ограничение выхода информации за пределы предприятия, что может быть реализовано несколькими способами, например введением должности цензора или предоставлением права отправлять документы в посторонние организации ограниченному кругу сотрудников. Вариант действий выбирает заказчик системы, исходя из степени закрытости сведений, хранимых и обрабатываемых СЭД.

Рассмотрим некоторые технические вопросы реализации обмена данными между серверами СЭД.

Для связи между серверными компьютерами может быть применено несколько низкоуровневых протоколов. Наиболее предпочтительным для целей передачи данных в этом случае является использование стандартных интернет-протоколов HTTP (обычно используемый интернет-браузерами) и SMTP (протокол электронной почты). К преимуществам первого можно отнести распространенность и простоту, к недостаткам — то, что он не обрабатывает ситуации отсутствия соединения и шифрования трафика, причем второй недостаток может быть устранен использованием протокола шифрования SSL.

Что касается почтового протокола SMTP, главное его достоинство как раз в возможности корректной работы при разрыве соединения, обеспечиваемой развитой инфраструктурой серверов электронной почты. Недостаток — сравнительно невысокая скорость обмена, вызванная наличием этой самой инфраструктуры. Что касается безопасности пе-

редаваемых данных, она может быть обеспечена шифрованием пересылаемых писем и приложенных файлов любыми криптосредствами.

Для передачи данных может быть использован сравнительно высокоуровневый протокол SOAP (Simple Object Access Protocol — простой протокол для доступа к объектам), основной особенностью которого является возможность применения для низкоуровневой передачи данных как SMTP, так и HTTP с SSL. Выбор между этими протоколами может быть сделан при внедрении системы с учетом требований конкретного заказчика.

Особенности обеспечения информационной безопасности электронного документооборота рассматриваются в следующем разделе.

6.2. Особенности защиты электронного документооборота

Внедрение системы электронного документооборота (СЭД) обеспечивает компании большую гибкость в обработке и хранении информации и заставляет сотрудников компании работать быстрее и с большей отдачей.

Спрос на системы электронного документооборота растет, и, по прогнозам экспертов, эта тенденция продолжится. В то же время применение СЭД порождает новые риски и пренебрежение защитой обязательно приведет к новым угрозам безопасности. Внедряя СЭД, нельзя забывать о безопасности корпоративной информационной системы.

Базовым элементом любой СЭД является документ; внутри системы это может быть, например, файл или запись в базе данных.

Говоря о защищенном документообороте, часто подразумевают именно защиту документов, защиту той информации, которую они в себе несут. Однако на самом деле нужно заботиться о защите всей системы электронного документооборота, а не только данных внутри нее. Это означает, что нужно защитить работоспособность СЭД, обеспечить быстрое восстановление после повреждений, сбоев и даже после уничтожения.

Поэтому к защите системы электронного документооборота необходим комплексный подход, который подразумевает защиту на всех уровнях СЭД, начиная от физических носителей информации, данных на них и заканчивая организационными мерами.

Таким образом, защита необходима, во-первых, аппаратным элементам системы. Это компьютеры, серверы, элементы компьютерной сети и сетевое оборудование.

Во-вторых, защита необходима файлам системы. Это файлы программного обеспечения и базы данных. В случае их незащищенности появляется возможность воздействия злоумышленника на файлы СЭД. Например, файлы базы данных могут быть скопированы злоумышленником или повреждены в результате сбоя операционной системы или оборудования.

В-третьих, необходимо защищать документы и информацию, находящиеся внутри системы.

Используя такой подход, можно построить систему, защищенную на всех уровнях, с рубежами обороны от угроз на каждом уровне. Стоимость такой защиты может сравняться со стоимостью самой СЭД, поэтому нужно искать разумный баланс между безопасностью и стоимостью.

Угрозы для СЭД

Угрозы для системы электронного документооборота могут быть классифицированы следующим образом:

- *угроза целостности* — повреждение и уничтожение информации, искажение информации — как ненамеренное в случае ошибок и сбоев, так и злоумышленное;
- *угроза конфиденциальности* — это любое нарушение конфиденциальности, в том числе кража, перехват информации, изменения маршрутов следования;
- *угроза работоспособности системы* — всевозможные угрозы, реализация которых приведет к нарушению или прекращению работы системы; сюда входят как умышленные атаки, так и ошибки пользователей, а также сбои в оборудовании и программном обеспечении.

Защита от этих угроз должна быть реализована в любой системе электронного документооборота. Упорядочение документооборота позволяет выстроить более качественную систему защиты.

Можно выделить несколько основных групп источников угроз: легальные пользователи системы, административный ИТ-персонал, внешние злоумышленники.

Согласно многочисленным исследованиям, от 70 до 80 % потерь от преступлений приходятся на атаки изнутри.

Пользователь системы является потенциальным злоумышленником, он может сознательно или несознательно нарушить конфиденциальность информации. Спектр возможных злоумышленных действий легальных пользователей достаточно широк — от скрепок в аппаратных частях системы до кражи информации с корыстной целью. При этом возможна реализация угроз в разных классах: угрозы конфиденциальности, целостности, работоспособности.

Особую группу составляет административный ИТ-персонал, или персонал службы ИТ-безопасности. Эта группа, как правило, имеет неограниченные полномочия и доступ к хранилищам данных, поэтому к ней нужно относиться с особым вниманием. Они не только имеют большие полномочия, но и наиболее квалифицированны в вопросах безопасности и информационных возможностей.

Состав внешних злоумышленников сугубо индивидуален. Это могут быть и конкуренты, и партнеры, и даже клиенты.

Средства защиты СЭД

Методы и средства защиты компьютеров, компьютерных сетей и сетевых устройств были рассмотрены в предыдущих главах. В данной главе рассмотрим более подробно средства, интегрированные в сами СЭД.

Любая защищенная СЭД должна иметь средства защиты для выполнения следующих функций:

- обеспечение сохранности документов;
- обеспечение безопасного доступа;
- обеспечение конфиденциальности;
- обеспечение подлинности документов;
- протоколирование действий пользователей.

Обеспечение сохранности документов

СЭД должна обеспечить сохранность документов от потери и порчи и иметь возможность их быстрого восстановления.

Согласно статистике, потери важной информации в 45 % случаев приходятся на физические причины (отказ аппаратуры, стихийные бедствия и т. п.), 35 % обусловлены ошибками пользователей и менее 20 % — действием вредоносных программ и злоумышленников.

Представители половины компаний, переживших потерю данных, заявляют, что причиной инцидента стал саботаж или халатное отношение сотрудников компании к правилам информационной политики компании, и только 20 % респондентов сообщили, что интеллектуальная собственность их компаний защищена должным образом. Что касается СЭД, то в эффективности ее защиты уверены только 24 % участников опроса.

Например, для СЭД, использующих базы данных Microsoft SQL Server или Oracle, предпочитают применять средства резервного копирования от разработчика СУБД (в данном случае от «Майкрософт» или Oracle). Иные системы имеют собственные подсистемы резервного копирования, разработанные непосредственно производителем СЭД.

Обеспечение безопасного доступа

Безопасный доступ к данным внутри СЭД обеспечивается аутентификацией и разграничением прав доступа к объектам.

Аутентификация. В СЭД могут использоваться различные методы аутентификации. Самый распространенный из них — применение многоразовых паролей. Шифрованные значения паролей обычно хранятся на сервере в специальной базе данных пользователей. Однако надежность данного метода сильно снижает человеческий фактор. Даже если пользователь использует правильно сгенерированный пароль, иногда его можно обнаружить записанным на листке бумаги в столе или под клавиатурой.

Часто полномочия пользователя подтверждаются специальным носителем информации. Существует множество решений для имущественной аутентификации пользователя: это USB-ключи, смарт-карты, магнитные карты, дискеты и компакт-диски. Здесь также не исключено влияние человеческого фактора, но злоумышленнику необходимо не только получить сам ключ, но и узнать PIN-код.

Надежным для проведения идентификации и последующей аутентификации является биометрический метод, при котором пользователь идентифицируется по своим биометрическим данным (это может быть отпечаток пальца, сканирование сетчатки глаза). Однако стоимость решения в этом случае выше, а современные биометрические технологии еще не настолько совершенны, чтобы избежать ложных срабатываний или отказов.

Важным параметром аутентификации является количество учитываемых факторов. Процесс аутентификации может быть однофакторным, двухфакторным и т. д. Возможно также комбинирование различных методов: парольного, имущественного и биометрического. Например, аутентификация может проходить при помощи пароля и отпечатка пальца (двухфакторный способ).

Разграничение прав доступа к объектам. Разграничение прав доступа к объектам системы электронного документооборота может быть реализовано исходя из различных принципов:

- задание пользователей и групп, имеющих право чтения, редактирования или удаления всего документа, включая присоединенные файлы и реквизиты;
- мандатный доступ по группам, когда доступ к данным предоставляется в соответствии с фиксированными уровнями полномочий групп пользователей;
- разграничение доступа к различным частям документов, например к разным присоединенным файлам, группам реквизитов, полям регистрационных карточек, поручениям по документу.

Среди методов разграничения доступа можно выделить:

- задание доступа на уровне серверной базы данных;
- ограничение доступа на интерфейсном уровне, когда ряд действий не может быть выполнен через пользовательский интерфейс, но доступен в случае написания отдельной программы.

Обеспечение конфиденциальности

Обеспечение конфиденциальности информации осуществляется с помощью криптографических методов защиты данных. Их применение позволяет не нарушить конфиденциальность документа даже в случае его попадания в руки стороннего лица.

Не стоит забывать, что любой криптографический алгоритм обладает таким свойством, как криптостойкость, т. е. и его защите есть предел. Нет шифров, которые нельзя было бы взломать, — это вопрос только

времени и средств. Те алгоритмы, которые еще несколько лет назад считались надежными, сегодня уже успешно взламываются.

Поэтому для обеспечения конфиденциальности следует убедиться, что за время, потраченное на взлом зашифрованной информации, она либо безнадежно устареет, либо средства, потраченные на ее взлом, превзойдут стоимость самой информации.

Кроме того, не следует забывать об организационных мерах защиты. Какой бы эффективной криптография ни была, ничто не помешает третьему лицу прочитать документ, например, стоя за плечом человека, который имеет к нему доступ, или расшифровать информацию, воспользовавшись ключом, лежащим в столе сотрудника.

Обеспечение подлинности документов

При организации электронного документооборота необходимо обеспечить юридическую значимость электронных документов в соответствии с российским законодательством. Эту задачу можно решить, используя систему электронной цифровой подписи (ЭЦП) и инфраструктуру управления открытыми ключами PKI.

Основной принцип работы ЭЦП основан на технологии шифрования с асимметричным ключом, при которой ключи для шифрования и расшифрования данных различны. Имеется закрытый ключ, который позволяет зашифровать информацию, и открытый ключ, при помощи которого можно эту информацию расшифровать, но с его помощью невозможно зашифровать эту информацию. Таким образом, владелец цифровой подписи должен владеть закрытым ключом и не допускать его передачу другим лицам, а открытый ключ может распространяться публично для проверки подлинности цифровой подписи, полученной при помощи закрытого ключа.

Подписать электронный документ с использованием ЭЦП может только обладатель закрытого ключа, а проверить наличие ЭЦП способен любой участник электронного документооборота, получивший открытый ключ, парный закрытому ключу отправителя. Успешная проверка ЭЦП показывает, что электронный документ подписан именно тем, от кого он исходит, и что он не был модифицирован после наложения ЭЦП.

Подтверждение принадлежности открытых ключей конкретным лицам осуществляет удостоверяющий центр инфраструктуры управления открытыми ключами PKI — специальная организация, которой доверяют все участники информационного обмена.

Обращение в удостоверяющий центр позволяет каждому участнику убедиться, что имеющиеся у него копии открытых ключей других участников (для проверки их ЭЦП) действительно принадлежат этим участникам.

Большинство производителей СЭД имеют встроенные в свои системы, собственноручно разработанные или партнерские средства для ис-

пользования ЭЦП, как, например, в системах Directum или «Евфрат-Документооборот». Такой тесной интеграции с ЭЦП немало способствовал и выход федерального закона об ЭЦП (№ 1-ФЗ от 10.01.2002), в котором электронная цифровая подпись была признана имеющей юридическую силу наряду с собственноручной подписью. Стоить заметить, что согласно законам РФ свою систему электронной цифровой подписи может разрабатывать только компания, имеющая на это соответствующую лицензию от ФСБ.

Протоколирование действий пользователей

Важным моментом в защите электронного документооборота является протоколирование действий пользователей. Его правильная реализация в системе позволяет отследить все неправомерные действия и найти виновника, а при оперативном вмешательстве даже пресечь попытку неправомерных или наносящих вред действий.

Такая возможность обязательно должна присутствовать в самой СЭД. Кроме того, дополнительно можно воспользоваться решениями сторонних разработчиков и партнеров, чьи продукты интегрированы с СЭД. Прежде всего, следует отметить СУБД и хранилища данных, любой подобный продукт крупных разработчиков, таких как «Майкрософт» или Oracle, наделен этими средствами. Также можно использовать возможности операционных систем по протоколированию действий пользователей.

Комплексный подход к защите электронного документооборота

При формировании защиты электронного документооборота необходимо объективно оценить возможные угрозы и риски СЭД и величину возможных потерь от реализованных угроз. Как уже отмечалось, защита СЭД не сводится только лишь к защите документов и разграничению доступа к ним.

Необходимо обеспечить защиту аппаратных средств системы, персональных компьютеров, принтеров и прочих устройств; защиту сетевой среды, в которой функционирует система; защиту каналов передачи данных и сетевого оборудования.

На каждом уровне защиты важную роль играет комплекс организационных мер (инструктаж, подготовка персонала к работе с конфиденциальной информацией).

Защита системы электронного документооборота должна быть комплексной.

О законодательном и нормативном регулировании

Российское законодательство начинает проявлять активный интерес к высоким технологиям и, в частности, к информатизации. Вопросы обеспечения безопасности электронного документооборота решаются

на основе законодательной и нормативной базы в области защиты информации.

К законодательной базе в первую очередь относятся:

- Закон РФ «Об информации, информатизации и защите информации»;
- Закон РФ «Об электронной цифровой подписи»;
- Государственная система сертификации продуктов защиты данных и лицензирования деятельности по предоставлению услуг в области защиты информации.

К нормативной базе относятся:

- стандарты криптографической защиты данных;
- требования и положения Гостехкомиссии РФ, касающиеся средств защиты информации от НСД.

Список законов и государственных стандартов, представленный здесь, не является полным; кроме указанных существует еще ряд законов, стандартов и требований ГТК РФ.

6.3. Защита баз данных

База данных представляет собой важнейший корпоративный ресурс, который должен быть надлежащим образом защищен с помощью соответствующих средств от любых умышленных или непредумышленных угроз.

Понятие защиты применимо не только к данным, хранящимся в базе данных. Защита базы данных должна охватывать используемое оборудование, программное обеспечение, персонал и собственно данные.

Обсудим проблемы защиты базы данных с точки зрения таких потенциальных опасностей:

- похищение и фальсификация данных;
- утрата конфиденциальности (нарушение тайны);
- нарушение неприкосновенности личных данных;
- нарушение целостности данных;
- потеря доступности данных.

Отмеченные опасности указывают основные направления, в которых нужно принимать меры, снижающие степень риска, т. е. потенциальную возможность потери или повреждения данных.

Похищение и фальсификация данных могут происходить не только в среде базы данных — вся организация так или иначе подвержена этому риску. Однако действия по похищению или фальсификации информации всегда совершаются людьми, поэтому основное внимание должно быть сосредоточено на сокращении общего количества удобных ситуаций для выполнения подобных действий.

Понятие конфиденциальности означает необходимость сохранения данных в тайне. Конфиденциальными считаются только те данные, ко-

торые являются важными для всей организации, тогда как понятие *неприкосновенности данных* касается требования защиты информации, принадлежащей отдельным сотрудникам. Следствием нарушения в системе защиты, вызвавшего потерю конфиденциальности данных, может быть утрата надежных позиций в конкурентной борьбе, тогда как следствием нарушения неприкосновенности личных данных могут стать судебные действия в отношении организации.

Нарушение целостности данных приводит к искажению или разрушению данных, что может иметь серьезные последствия для дальнейшей работы организации. В настоящее время множество организаций функционируют в непрерывном режиме, предоставляя свои услуги клиентам 24 часа в сутки и 7 дней в неделю.

Потеря доступности данных будет означать, что либо данные, либо система, либо и то и другое одновременно окажутся недоступными пользователям, а это может подвергнуть опасности финансовое положение организации.

Цель защиты базы данных — минимизировать потери, вызванные перечисленными и другими возможными событиями.

Принимаемые решения должны обеспечивать эффективное возмещение понесенных затрат и исключать излишнее ограничение предоставляемых пользователям возможностей [34, 62].

6.3.1. Основные типы угроз

Угроза может быть вызвана ситуацией (или событием), способной принести ущерб организации, причиной которой может служить человек, происшествие или стечение обстоятельств.

Ущерб может быть материальным (например, потеря оборудования, программного обеспечения или данных) или нематериальным (например, потеря доверия партнеров или клиентов).

Перед каждой организацией стоит проблема выявления всех возможных опасностей, что является весьма непростой задачей. Поэтому на выявление хотя бы важнейших угроз может потребоваться достаточно много времени и усилий.

Любая угроза должна рассматриваться как потенциальная возможность нарушения системы защиты, которая в случае успешной реализации может оказать то или иное негативное влияние.

Приведем некоторые примеры возможных угроз для баз данных:

- похищение данных, программ и оборудования;
- несанкционированное изменение или копирование данных;
- просмотр и раскрытие засекреченных данных;
- создание «лазеек» в системе;
- внедрение компьютерных вирусов;
- использование прав доступа другого лица;
- ввод некорректных данных;
- пожары, наводнения, диверсии и др.

6.3.2. Методы и средства защиты СУБД

В отношении угроз, которые могут оказать отрицательное воздействие на работу базы данных, должны быть приняты контрмеры, начиная от физического контроля и заканчивая административно-организационными процедурами. Следует отметить, что общий уровень защищенности СУБД определяется возможностями используемой операционной системы, поскольку работа этих двух компонентов тесно связана между собой.

Для обеспечения информационной безопасности СУБД применяются следующие методы и средства защиты:

- авторизацию пользователей;
- применение представлений;
- шифрование данных;
- поддержку целостности данных;
- резервное копирование и восстановление данных;
- применение RAID-массивов.

Авторизация пользователей

Под авторизацией понимают предоставление прав (или привилегий), позволяющих их владельцу иметь законный доступ к системе или к ее объектам. Термин «владелец» в приведенном выше определении может означать пользователя — человека или программу. Термин «объект» может означать таблицу данных, представление, приложение, процедуру или другой объект, который может быть создан в рамках системы.

Средства авторизации пользователей могут быть встроены непосредственно в программное обеспечение и управлять не только предоставленными пользователям правами доступа к системе или объектам, но и набором операций, которые пользователи могут выполнять с каждым доступным им объектом. По этой причине механизм авторизации часто называют средствами управления доступом.

За предоставление пользователям доступа к компьютерной системе обычно отвечает системный администратор, в обязанности которого входит создание учетных записей пользователей. Каждому пользователю присваивается уникальный идентификатор, который используется операционной системой для определения того, кто есть кто.

С каждым идентификатором связывается определенный пароль, выбираемый пользователем и известный операционной системе. При регистрации пользователь должен предоставлять системе свой пароль для выполнения проверки (аутентификации) того, является ли он тем, за кого себя выдает. Подобная процедура позволяет организовать контролируемый доступ к компьютерной системе, но необязательно предоставляет право доступа к СУБД или иной прикладной программе. Для получения пользователем права доступа к СУБД может использоваться

отдельная процедура. Существует ряд других решений для аутентификации пользователя: это USB-ключи, смарт-карты, магнитные карты, цифровые сертификаты, средства биометрической аутентификации (см. главу 5).

Ответственность за предоставление прав доступа к СУБД обычно несет администратор базы данных (АБД), в обязанности которого входит создание отдельных идентификаторов пользователей в среде самой СУБД.

В некоторых СУБД ведется список идентификаторов пользователей и связанных с ними паролей, отличающийся от аналогичного списка, поддерживаемого операционной системой.

Привилегии. Как только пользователь получает право доступа к СУБД, ему могут автоматически предоставляться различные привилегии, связанные с его идентификатором. В частности, эти привилегии могут включать *разрешение на доступ к определенным базам данных, таблицам и представлениям, а также на создание этих объектов или же право вызывать на выполнение различные утилиты СУБД.*

Привилегии предоставляются пользователям, чтобы они могли выполнять задачи, которые относятся к кругу их должностных обязанностей. Предоставление излишних или ненужных привилегий может привести к нарушению защиты, поэтому пользователь должен получать только такие привилегии, без которых он не имеет возможности выполнять свою работу.

Некоторые типы СУБД функционируют как *закрытые системы*, поэтому пользователям помимо разрешения на доступ к самой СУБД потребуется иметь отдельные разрешения и на доступ к конкретным ее объектам. Эти разрешения выдаются либо АБД, либо владельцами определенных объектов системы.

В противоположность этому *открытые системы* по умолчанию предоставляют пользователям, прошедшим проверку их подлинности, полный доступ ко всем объектам базы данных. В этом случае привилегии устанавливаются посредством явной отмены тех или иных прав конкретных пользователей.

Права владения и привилегии. Как правило, *владение некоторым объектом СУБД предоставляет его владельцу весь возможный набор привилегий в отношении этого объекта.* Это правило применяется ко всем авторизованным пользователям, получающим права владения определенными объектами.

Любой вновь созданный объект автоматически передается во владение его создателю, который и получает весь возможный набор привилегий для данного объекта. Хотя при этом пользователь может быть владельцем некоторого представления, единственной привилегией, которая будет предоставлена ему в отношении этого объекта, может оказаться правом выборки данных из тайного представления. Причина подобных ограничений состоит в том, что указанный пользователь имеет ограниченный набор прав в отношении базовых таблиц созданного им представления.

Принадлежащие владельцу привилегии могут быть переданы им другим авторизованным пользователям. Например, владелец нескольких таблиц базы данных может предоставить другим пользователям право выборки информации из этих таблиц, но не позволить им вносить в таблицы какие-либо изменения.

В языке SQL предусмотрено, что, если пользователь передает какие-либо привилегии, он может указать, приобретает ли получатель этих привилегий право передавать эти привилегии другим пользователям.

Если СУБД поддерживает несколько различных типов идентификаторов авторизации, с каждым из существующих типов могут быть связаны различные приоритеты. В частности, если СУБД поддерживает использование идентификаторов отдельных пользователей и групп, то, как правило, идентификатор пользователя будет иметь более высокий приоритет, чем идентификатор группы.

В некоторых СУБД пользователю разрешается указывать, под каким идентификатором он намерен работать далее, — это целесообразно в тех случаях, когда один и тот же пользователь может являться членом сразу нескольких групп.

Применение представлений

Представление — динамический результат одной или нескольких реляционных операций с базовыми отношениями с целью создания некоторого иного отношения.

Представление является *виртуальным отношением*, которое реально в базе данных не существует, но создается по требованию отдельного пользователя в момент поступления этого требования.

Механизм представлений служит мощным и гибким инструментом организации защиты данных, позволяющим скрывать от определенных пользователей некоторые части базы данных. В результате пользователи не будут иметь никаких сведений о существовании любых атрибутов или строк данных, которые не доступны через представления, находящиеся в их распоряжении.

Представление может быть определено на базе нескольких таблиц, после чего пользователю будут предоставлены необходимые привилегии доступа к этому представлению, но не к базовым таблицам. В данном случае использование представления устанавливает более жесткий механизм контроля доступа, чем обычное предоставление пользователю тех или иных прав доступа к базовым таблицам.

Шифрование данных

Традиционным способом обеспечения конфиденциальности данных является их шифрование. В процессе длительной эволюции серверов баз данных шифрование данных не применялось в течение многих

лет. Шифрование данных в базах данных стало возможным только в последние годы, когда мощность процессоров достигла определенного уровня.

В современных СУБД для шифрования данных в таблицах используется симметричное шифрование. Самым простым вариантом для пользователя является *прозрачное шифрование данных* (Transparent Data Encryption). Эта технология базируется на управлении ключами системными средствами.

Ключевая информация, используемая для шифрования данных, хранится в специальном файле-«бумажнике» (Wallet). Для доступа к бумажнику определен пароль walletpsw. Для того чтобы открыть бумажник, необходимо предъявить файл и указать правильный пароль. Следует отметить, что в реальной системе хранить критически важную информацию в общеизвестном месте — не самое лучшее решение.

Изменение таблицы, связанное с шифрованием столбца, требует наличия открытого бумажника. Для доступа к информации, хранящейся в зашифрованном столбце, также необходимо открыть бумажник. Бумажник открывается только один раз любым из пользователей, имеющих право на выполнение операции. Естественно, что после выполнения операций с закрытыми столбцами бумажник рекомендуется закрыть.

Важно отметить, что, после того как законный пользователь открыл бумажник, содержимое таблицы становится доступным всем пользователям, имеющим право доступа к данным таблицы. Отмеченный факт существенно ограничивает область применения технологии прозрачного шифрования для систем с высокими требованиями к информационной безопасности.

В ряде случаев более предпочтительным оказывается выбор технологии *шифрования данных с явным заданием ключа пользователем*. Использование данной технологии предполагает наличие процедуры управления ключами. Администратор безопасности должен определить технологию генерации и распределения ключей, процедуры распределения и отзыва ключей (в случае их компрометации), процедуры управления резервными копиями ключей. При этом целесообразно использовать технику хранения пользователем ключевой информации на внешнем носителе. В качестве внешнего носителя часто используют устройство хранения данных на флэш-памяти.

Отсутствие отработанных способов решения перечисленных задач или небрежное их выполнение может привести к серьезным негативным последствиям. Потеря ключа может быть связана, например, с разрушением физического средства его хранения. Возможна утеря физического средства хранения информации. В любом случае происходит необратимая потеря данных. Современные средства криптографии обладают высокой стойкостью, и потеря ключа в большинстве случаев означает потерю данных.

В процедурах шифрования могут использоваться криптографические алгоритмы блочного шифрования DES, 3-DES, AES и алгоритм

потокового шифрования RC4. Алгоритмы блочного шифрования могут использоваться в четырех режимах:

- режим электронной кодовой книги ECB (Electronic Code Book);
- режим сцепления блоков CBC (Cipher Block Chaining);
- режим обратной связи по шифртексту CFB (Cipher Feed Back);
- режим обратной связи по выходу OFB (Output Feed Back).

Шифрование может также использоваться для защиты данных при их передаче по линиям связи.

Поддержка целостности данных

Средства поддержки целостности данных также вносят определенный вклад в общую защищенность базы данных, поскольку они должны предотвратить переход данных в несогласованное состояние, а значит, исключить угрозу получения неправильных результатов.

Средства обеспечения целостности баз данных включают автоматическую поддержку некоторой системы правил, описывающих допустимость и достоверность хранимых и вводимых значений [62]. Реляционная модель включает некоторые характерные правила, вытекающие из ее существа: ограничения домена и ограничения таблицы.

Целостность домена предполагает, что допустимое множество значений каждого атрибута является формально определенным. Существуют формальные способы проверки того, что конкретное значение атрибута в базе данных является допустимым. Строка не будет вставлена в таблицу, пока каждое из значений ее столбцов не будет находиться в соответствующем домене (множестве допустимых значений).

Целостность таблицы означает, что каждая строка в таблице должна быть уникальной. Хотя не все СУБД промышленного уровня требуют выполнения такого ограничения, возможность уникальной идентификации каждой строки представляется необходимой для большинства реальных приложений.

Ограничения целостности позволяют гарантировать, что требования к данным будут соблюдаться независимо от способа их загрузки или изменения.

Резервное копирование и восстановление

Резервное копирование — периодически выполняемая процедура получения копии базы данных и ее файла журнала (а также, возможно, программ) на носителе, хранящемся отдельно от системы.

Любая современная СУБД должна предоставлять средства резервного копирования, позволяющие восстанавливать базу данных в случае ее разрушения. Кроме того, рекомендуется создавать резервные копии базы данных и ее файла журнала с некоторой установленной периодичностью, а также организовывать хранение созданных копий в местах, обеспеченных необходимой защитой.

В случае аварийного отказа, в результате которого база данных становится непригодной для дальнейшей эксплуатации, резервная копия и зафиксированная в файле журнала оперативная информация используются для восстановления базы данных до последнего согласованного состояния.

Ведение журнала представляет собой процедуру создания и обслуживания файла журнала, содержащего сведения обо всех изменениях, внесенных в базу данных с момента создания последней резервной копии, и предназначенного для обеспечения эффективного восстановления системы в случае ее отказа.

СУБД должна предоставлять средства ведения системного журнала, в котором будут фиксироваться сведения обо всех изменениях состояния базы данных и о ходе выполнения текущих транзакций, что необходимо для эффективного восстановления базы данных в случае отказа.

Преимущества использования подобного журнала заключаются в том, что в случае нарушения работы или отказа СУБД можно будет восстановить до последнего известного согласованного состояния, воспользовавшись последней созданной резервной копией базы данных и оперативной информацией, содержащейся в файле журнала. Если в отказавшей системе функция ведения системного журнала не использовалась, базу данных можно будет восстановить только до того состояния, которое было зафиксировано в последней созданной резервной копии. Все изменения, внесенные в базу данных после создания последней резервной копии, будут потеряны.

Применение RAID-массивов

Аппаратное обеспечение, на котором эксплуатируется СУБД, должно быть отказоустойчивым. Это означает, что СУБД должна продолжать работать даже при отказе аппаратных компонентов. Для этого необходимо иметь избыточные компоненты, которые могут быть объединены в систему, сохраняющую свою работоспособность при отказе одного или нескольких компонентов.

К числу основных аппаратных компонентов, которые должны быть отказоустойчивыми, относятся дисковые накопители, дисковые контроллеры, процессоры, источники питания и вентиляторы охлаждения. Дисковые накопители являются наиболее уязвимыми среди всех аппаратных компонентов и характеризуются самыми низкими показателями непрерывной работы между отказами.

Одним из решений этой проблемы является применение технологии RAID. Первоначально эта аббревиатура расшифровывалась как Redundant Array of Inexpensive Disks (Массив недорогих дисковых накопителей с избыточностью), но в дальнейшем букву I в этой аббревиатуре стали рассматривать как сокращение от Independent (независимый).

RAID-массив представляет собой массив дисковых накопителей большого объема, состоящий из нескольких независимых дисков, со-

вместное функционирование которых организовано таким образом, что при этом повышается надежность и вместе с тем увеличивается производительность [34, 47].

Производительность увеличивается благодаря полосовому распределению данных. Данные на дисках распределяются по сегментам, представляющим собой разделы дисков равного размера (этот размер называется *единицей полосового распределения*), которые распределяются по нескольким дискам и обеспечивают прозрачный доступ. В результате такой массив становится аналогичным одному крупному быстродействующему диску, но фактически данные в нем распределены по нескольким дискам меньшего объема.

Полосовое распределение обеспечивает повышение производительности ввода-вывода, поскольку позволяет одновременно выполнять несколько операций ввода-вывода (на разных дисках). Наряду с этим полосовое распределение данных позволяет равномерно распределять нагрузку между дисками.

Повышенная надежность RAID-массива обеспечивается благодаря дублированию данных (такие дубликаты называются *зеркальными копиями*) и хранению на дисках избыточной информации, сформированной с использованием схем контроля четности или схем исправления ошибок, таких как корректирующий код Рида—Соломона (Reed—Solomon) [55].

В схеме контроля четности каждый байт должен иметь связанный с ним бит четности, который принимает значение 0 или 1 в зависимости от того, является ли четным или нечетным количество битов 1 в байте, которому соответствует этот бит контроля четности. Если в контролируемом байте некоторые биты будут искажены, значение бита четности не совпадет со значением, соответствующим новому составу битов 1 в этом байте. Аналогичным образом, при искажении хранимого бита контроля четности он не будет соответствовать данным в байте, что позволит обнаружить ошибку.

С другой стороны, схемы корректировки ошибок предусматривают хранение двух или больше дополнительных битов и позволяют восстанавливать первоначальные данные, если один из битов будет искажен.

Схемы контроля четности и корректировки ошибок могут применяться при полосовом распределении данных по дискам.

В RAID-массивах используются различные сочетания описанных выше методов повышения производительности и надежности, получившие название уровней RAID. Эти уровни перечислены ниже.

- *RAID 0* (неизбыточный массив). На этом уровне не применяется дублирование данных и поэтому обеспечивается наивысшая производительность записи, поскольку не приходится копировать по дискам обновляемые данные. Полосовое распределение данных осуществляется на уровне дисковых блоков;
- *RAID 1* (массив с зеркальным отображением). На этом уровне ведутся две идентичные (зеркальные) копии данных на разных дисках. Для обеспечения сохранности данных на случай отказа диска запись на разные диски в некоторых вариантах реализации такого массива

не выполняется одновременно. Этот вариант организации хранения данных во внешней памяти является наиболее дорогостоящим;

- *RAID 0 + 1* (неизбыточный массив с зеркальным отображением). На этом уровне применяется сочетание методов полосового распределения и зеркального отображения данных;
- *RAID 2* (массив с применением кодов корректировки ошибок, хранящихся во внешней памяти). На этом уровне единицей полосового распределения является один бит и для реализации схемы избыточности применяются корректирующие коды Хэмминга;
- *RAID 3* (массив, обеспечивающий контроль четности с чередованием битов). На этом уровне предусматривается хранение избыточных данных (представляющих собой информацию контроля четности) на отдельном диске массива. Эта информация может применяться для восстановления данных, хранящихся на других дисках, в случае отказа этих дисков. На этом уровне используется меньший дополнительный объем пространства внешней памяти по сравнению с уровнем RAID 1, но доступ к диску с информацией контроля четности может стать узким местом, ограничивающим производительность;
- *RAID 4* (массив, обеспечивающий контроль четности с чередованием блоков). На этом уровне единицей полосового распределения является блок диска; блоки с информацией контроля четности хранятся на ином диске, чем соответствующие блоки данных с нескольких других дисков. При отказе одного из дисков с данными блок контроля четности может применяться в сочетании с соответствующими блоками с других дисков для восстановления данных, которые хранились на отказавшем диске;
- *RAID 5* (массив, обеспечивающий контроль четности с чередованием блоков и распределением информации контроля четности). На этом уровне информация контроля четности применяется в качестве избыточной и обеспечивающей восстановление первоначальных данных по такому же принципу, как в массиве RAID 3; но данные контроля четности распределяются с помощью метода полосового распределения по всем дискам таким же образом, как происходит распределение исходных данных. Это позволяет устранить узкое место, возникающее, если вся информация контроля четности хранится на одном диске;
- *RAID 6* (массив с избыточностью P + Q). Этот уровень аналогичен уровню RAID 5, но предусматривает хранение дополнительных избыточных данных для защиты от отказа сразу нескольких дисков. При этом вместо информации контроля четности используются коды исправления ошибок.

Например, корпорация Oracle рекомендует использовать уровень RAID 1 для файлов журнала восстановления. Для файлов базы данных рекомендуется применение уровня RAID 5, если он обеспечивает приемлемые задержки при записи, а в ином случае рекомендуется уровень RAID 1 или RAID 0 + 1.

6.3.3. Средства защиты СУБД Microsoft Access

СУБД Microsoft Access 2000 предоставляет следующие два метода защиты базы данных:

- установку пароля, который применяется при открытии базы данных (это средство в терминологии Microsoft Access называется *защитой системы*);
- применение средств защиты на уровне пользователя, которые могут служить для определения тех частей базы данных, где пользователь может выполнять операции чтения или обновления (это средство в терминологии Microsoft Access называется *защитой данных*).

Рассмотрим, как эти механизмы защиты реализованы в СУБД Microsoft Access [34].

Установка пароля

Самым простым методом защиты является установка пароля, применяемого для открытия базы данных. После установки пароля (пункты меню **Сервис** ⇒ **Защита** ⇒ **Задать пароль базы данных**) при любой попытке открыть базу данных на экране появляется диалоговое окно с приглашением ввести пароль. Разрешение открыть базу данных получают только те пользователи, которые вводят правильный пароль.

Этот метод является надежным, поскольку СУБД Microsoft Access шифрует пароль таким образом, чтобы его нельзя было определить, непосредственно считывая файл базы данных, но после открытия базы данных все объекты, содержащиеся в ней, становятся доступными для пользователя.

Защита на уровне пользователя

Средства защиты на уровне пользователя в СУБД Microsoft Access аналогичны средствам, которые применяются в большинстве сетевых систем. При запуске программы Microsoft Access пользователи должны указать свой идентификатор и ввести пароль.

В файле с информацией о рабочих группах программы Microsoft Access пользователи обозначаются как члены некоторой группы. В СУБД Access предусмотрены по умолчанию две группы; администраторы (группа **Admins**) и пользователи (группа **Users**), но могут быть определены и дополнительные группы.

Группам и пользователям предоставляются права доступа, которые позволяют регламентировать перечень допустимых для них операций с каждым объектом базы данных. Для этого применяется диалоговое окно **Разрешения**.

В табл. 6.1 приведен перечень прав доступа, которые могут быть установлены в СУБД Microsoft Access.

Таблица 6.1. **Права доступа в СУБД Microsoft Access**

Права доступа	Допустимые операции
Открытие/запуск	Открытие базы данных, формы, отчета или вызов макрокоманды на выполнение
Монопольный доступ	Открытие базы данных с исключительными правами доступа
Чтение макета	Просмотр объектов в представлении макета
Изменение макета	Просмотр, изменение и удаление объектов базы данных
Администратора	Применительно к базам данных: установка пароля базы данных, копирование базы данных и изменение сценариев запуска. Применительно к объектам базы данных: полный доступ, в том числе возможность назначать права доступа
Чтение данных	Просмотр данных
Обновление данных	Просмотр и изменение данных (но не вставка и удаление)
Вставка данных	Просмотр и вставка данных (но не изменение и удаление)
Удаление данных	Просмотр и удаление данных (но не вставка и изменение)

6.3.4. Средства защиты СУБД Oracle

В предыдущем разделе описаны два типа средств защиты в СУБД Microsoft Access: защита системы и защита данных. В данном разделе показано, как эти два типа средств защиты реализованы в СУБД Oracle.

Как и в СУБД Access, одна из форм защиты системы, применяемая в СУБД Oracle, предусматривает реализацию стандартного механизма проверки идентификатора и пароля пользователя, в соответствии с которым пользователь должен ввести действительный идентификатор и пароль и только после этого получить доступ к базе данных [34, 62].

При каждой попытке пользователя подключиться к базе данных открывается диалоговое окно **Connect** (Подключение) или **Log On** (Вход) с приглашением ввести идентификатор и пароль пользователя для доступа к указанной базе данных.

Привилегии

Привилегия представляет собой право выполнять операторы SQL определенного типа или обращаться к объектам другого пользователя. Ниже приведены примеры некоторых привилегий Oracle, которые позволяют выполнять определенные действия.

- подключение к базе данных (открытие сеанса);
- создание таблицы;
- выборка строк из таблицы другого пользователя.

В СУБД Oracle предусмотрены две категории привилегий:

- системные привилегии;
- привилегии на объекты.

Системные привилегии

Системная привилегия представляет собой право выполнять определенные действия или проводить операции с любыми объектами схемы определенного типа. Например, к системным относятся привилегии на создание табличных пространств и учетных записей пользователей базы данных.

В СУБД Oracle предусмотрено свыше 80 системных привилегий. Системные привилегии можно предоставлять пользователям и ролям (которые рассматриваются ниже) или отзывать эти привилегии с использованием любого из следующих средств:

- диалоговые окна **Grant System Privileges/Roles** (Предоставление системных привилегий/ролей) и **Revoke System Privileges/Roles** (Отзыв системных привилегий/ролей) менеджера безопасности Oracle Security Manager;
- операторы `GRANT` и `REVOKE` языка SQL.

Предоставлять или отзывать системные привилегии могут только пользователи, которым предоставлена специальная системная привилегия с помощью конструкции `ADMIN OPTION`, или пользователи с системной привилегией `GRANT ANY PRIVILEGE`.

Привилегии на объекты

Привилегией на объект является привилегия или право выполнять определенное действие с конкретной таблицей, представлением, последовательностью, процедурой, функцией или пакетом.

Для работы с объектами разных типов предоставляются различные привилегии на объекты. Например, одной из привилегий на объект является право удалять строки из таблицы Staff.

С некоторыми объектами схемы (такими как кластеры, индексы и триггеры) не связаны привилегии на объекты; применение этих объектов регламентируется с помощью системных привилегий. Например, чтобы внести изменения в кластер, пользователь должен быть владельцем этого кластера или иметь системную привилегию `ALTER ANY CLUSTER`.

Пользователь автоматически приобретает все привилегии на объекты, содержащиеся в его схеме. Кроме того, пользователь может предоставить любому другому пользователю или роли привилегии на любые принадлежащие ему объекты схемы. Если в операторе SQL, применяемом для предоставления такой привилегии, включена опция `WITH GRANT OPTION` (оператора `GRANT`), лицо, получившее привилегию на объект, может предоставить ее другому пользователю; в противном слу-

чае он может использовать полученную привилегию, но не имеет право предоставлять ее другим пользователям. В табл. 6.2 показаны привилегии на такие объекты, как таблицы и представления.

Таблица 6.2. **Допустимые действия с таблицами и представлениями, права на выполнение которых предоставляются с помощью различных привилегий на объекты**

Привилегия на объект	Таблица	Представление
ALTER	Изменять определение таблицы с помощью оператора ALTER TABLE	Какие-либо действия не предусмотрены
DELETE	Удалять строки из таблицы с помощью оператора DELETE. **Примечание.** Наряду с привилегией DELETE должна быть предоставлена привилегия SELECT	Удалять строки из представления с помощью оператора DELETE
INDEX	Создавать индекс в таблице с помощью оператора CREATE INDEX	Какие-либо действия не предусмотрены
INSERT	Вводить новые строки в таблицу с помощью оператора INSERT	Вводить новые строки в представление с помощью оператора INSERT
REFERENCES	Создавать ограничение, которое ссылается на таблицу. Эта привилегия не может быть предоставлена роли	Какие-либо действия не предусмотрены
SELECTa	Запрашивать данные в таблице с помощью оператора SELECT	Запрашивать данные в представлении с помощью оператора SELECT
UPDATE	Модифицировать данные в таблице с помощью оператора UPDATE. **Примечание.** Наряду с привилегией UPDATE должна быть предоставлена привилегия SELECT	Изменять данные в представлении с помощью оператора UPDATE

Роли

Пользователь может получить привилегию двумя способами:

- привилегии могут предоставляться пользователям явным образом. Например, пользователю Beech может быть явно предоставлена привилегия вставлять строки в таблицу PropertyForRent: `GRANT INSERT ON PropertyForRent TO Beech;`
- привилегии могут также предоставляться некоторой *роли* (так называется именованная группа привилегий), а затем эта роль может предоставляться одному или нескольким пользователям. Например, привилегии на выборку, вставку и обновление строк в таблице `PropertyForRent` могут быть предоставлены роли `Assistant`, а эта роль, в свою очередь, — предоставлена пользователю Beech. Любой пользователь может иметь доступ к нескольким ролям,

а нескольким пользователям могут быть назначены одинаковые роли. Поскольку роли позволяют проще и лучше управлять привилегиями, то привилегии, как правило, должны предоставляться ролям, а не отдельным пользователям.

6.3.5. Защищенный доступ к базам данных

В предыдущих разделах было показано, что СУБД от ведущих мировых производителей имеют встроенные механизмы защиты. Они позволяют:

- авторизовать пользователей при доступе к БД;
- разграничивать права пользователей на управление данными (например, одни пользователи могут только просматривать БД, а другие — вносить в них добавления и изменения);
- разграничивать права пользователей на администрирование СУБД (операции по удалению старых или добавлению новых пользователей БД);
- разграничивать доступ пользователей к информации, хранящейся в БД.

Эти механизмы защиты позволяют обеспечить минимальный уровень безопасности.

Если администратор безопасности использует все перечисленные механизмы защиты, этого недостаточно для того, чтобы быть уверенным в безопасности своих компьютерных систем и обрабатываемых в них данных, по следующим причинам:

- пользователи базы данных, в том числе и ее администратор, могут назначить себе слабые пароли, которые легко подобрать. Кроме того, в некоторых СУБД аутентификационные данные администратора заложены на уровне программного кода и не могут быть изменены, хотя именно по этой причине они общеизвестны;
- администраторы БД порой несвоевременно удаляют старые учетные записи, например, при увольнении сотрудников, и неиспользуемые пароли остаются действительными еще в течение долгого времени;
- любая СУБД — это всего лишь программа, которую писали люди. Людям свойственно ошибаться. Ошибки в программном обеспечении могут при определенных условиях заставить программу функционировать неправильно. Такие ошибки называют уязвимостями. Именно ими и пользуются хакеры для проведения своих атак;
- хакерские атаки не всегда могут быть направлены непосредственно на СУБД. Любая база данных функционирует на платформе определенной операционной системы, которая тоже может иметь уязвимые места. Если злоумышленник сможет получить контроль над самим сервером, то все встроенные в СУБД механизмы безопасности будут практически бесполезны;

- целью злоумышленника не всегда является получение доступа к информации. Порой больше убытков может принести не разглашение информации, а недоступность для клиентов самого сервиса БД (например, простой системы продажи авиабилетов);
- никогда нельзя быть уверенным в том, что выданным администратором паролем будет пользоваться один человек и что этот пароль не станет достоянием других людей;
- информация, которая хранится и обрабатывается в базах данных, может быть конфиденциальной. Поэтому следует позаботиться о защите ее от перехвата в каналах связи.

Для обеспечения надежной защиты базы данных необходимо предпринять следующие меры (рис. 6.1):

1. Следует поместить серверы, на которых размещается БД, в отдельный сегмент сети и защитить вход в него межсетевым экраном. На межсетевом экране нужно задать правила, которые закроют пользователям сервиса баз данных доступ ко всему, кроме этих баз. Это существенно снизит риск того, что система будет взломана.

2. Чтобы защититься от уязвимостей, которыми могут воспользоваться легальные пользователи БД, необходимо установить систему обнаружения атак. Она позволит обнаруживать возможную несанкционированную сетевую активность в пределах разрешенных протоколов. Прослушивая сетевой трафик и сопоставляя его с базой сигнатур атак, сетевой сенсор обнаруживает различные нарушения политики безопасности. Использование системы обнаружения атак, разработанной с учетом специфики СУБД, позволяет дополнительно повысить уровень защищенности данных.

3. Контролировать деятельность администратора на предмет правильного управления настройками СУБД позволит система анализа за-

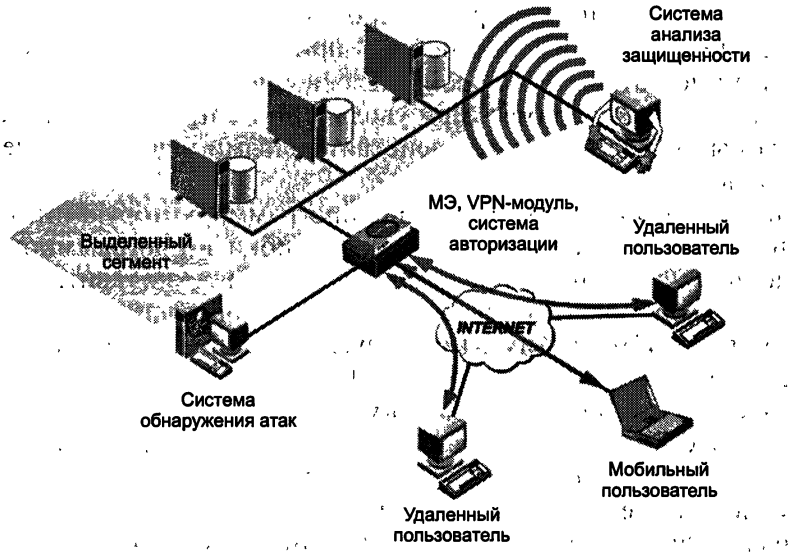


Рис. 6.1. Схема защищенного доступа к базам данных

щищенности. Она вовремя обнаружит неправильно назначенные права доступа к таблицам и процедурам, выявит слабые пароли, обнаружит неиспользуемые учетные записи и т. п. Кроме того, она найдет в СУБД известные ей уязвимости и выдаст рекомендации по их устранению.

4. Защитить информацию от перехвата, а учетные записи — от возможного тиражирования помогут средства VPN. Благодаря использованию цифровых сертификатов можно выдавать пользователям не пароли для доступа, а персональные сертификаты на различных носителях, которые не подлежат копированию [97].

Это обеспечит:

- строгую криптографическую аутентификацию удаленных пользователей;
- защиту данных, передаваемых в пределах рабочего сеанса;
- невозможность осуществить двойной вход в систему с одним набором учетных данных.

6.4. Защита корпоративного почтового документооборота

Эффективная деятельность любого современного предприятия немыслима без наличия электронного документооборота. Работа с документами в электронной форме позволяет быстро и удобно хранить, обрабатывать и передавать их в рамках корпоративной информационной системы (ИС). Перечисленные функции, как правило, выполняет почтовая система, являющаяся неотъемлемой частью всякого электронного документооборота [74]. Она включает в себя такие базовые элементы, как почтовые клиенты и почтовые серверы. Пример обобщенной архитектуры почтовой системы приведен на рис. 6.2.

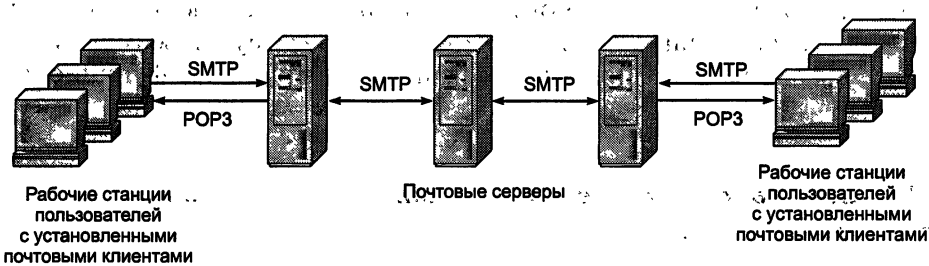


Рис. 6.2. Обобщенная архитектура электронной почтовой системы

Почтовые клиенты представляют собой ПО, устанавливаемое на рабочих станциях пользователей ИС. С помощью почтовых клиентов формируют, отправляют и получают электронные документы. Наиболее распространенными примерами почтовых клиентских программ являются Outlook компании «Майкрософт», а также The Bat! компании Rit Labs.

Почтовый сервер — это ПО, которое устанавливается на выделенном серверном ресурсе. Посредством почтового клиента пользователь формирует документ и через механизм SMTP (Simple Mail Transfer Protocol) передает его на почтовый сервер для отправки адресату. Последний, используя свой почтовый клиент, подключается к почтовому серверу и загружает документ на ПК. Получение электронной почты осуществляется по протоколу POP3 (Post Office Protocol, версия 3). Для взаимодействия же самих почтовых серверов между собой применяется протокол SMTP. Почтовыми серверами являются продукт Exchange компании «Майкрософт» и свободно распространяемое ПО sendmail.

Почтовая система, используемая в качестве основы электронного документооборота, обладает рядом преимуществ, основными из которых являются популярность данного сервиса среди пользователей компьютерных систем, быстрота доставки сообщений (электронная почта из России в США доставляется в среднем за 2 мин), а также низкая стоимость использования в сравнении с традиционной телефонной и факсимильной связью.

Следует, однако, иметь в виду, что любая почтовая система потенциально подвержена целому ряду угроз, которые способны привести к нарушению конфиденциальности, целостности или доступности информации. При этом угрозы безопасности системы могут исходить как со стороны внутренних пользователей, так и извне, например из сети Интернет.

Угрозы информационной безопасности воплощаются в реальных атаках злоумышленников. Объектами этих атак могут быть почтовые серверы, рабочие станции пользователей, а также информация, передаваемая между ними. Так, атакующий может поставить себе цель получить доступ к содержимому передаваемых почтовых сообщений и изменять его. Другой пример информационных атак — вторжение в ИС путем внедрения вирусов через почтовую систему.

С учетом вышеизложенного рассмотрим существующие методы и средства, позволяющие защитить почтовую систему от возможных угроз, и, насколько это возможно, проиллюстрируем их функциональность.

6.4.1. Защита каналов сетевого взаимодействия почтовых клиентов и серверов

Известно, что в почтовых протоколах SMTP и POP3 нет встроенных механизмов защиты передаваемых данных. Поэтому у злоумышленника появляется неплохая возможность реализовать атаку, направленную на нарушение конфиденциальности и/или целостности пакетов данных, передаваемых посредством этих протоколов.

Защититься от атак подобного типа можно с помощью технологии VPN, позволяющей организовать между хостами ИС зашифрованные каналы связи. При этом управление защищенными сетевыми соедине-

ниями осуществляется с помощью специализированных криптопротоколов. Последние реализуются на различных уровнях модели взаимодействия открытых систем (см. главу 9).

Виртуальные частные сети могут быть развернуты на базе сетевых ОС со встроенной VPN-функциональностью; активного сетевого оборудования, ПО которого поддерживает функции VPN; специализированного программно-аппаратного обеспечения, предназначенного для криптографической защиты информации.

Если средства защиты этого типа выполнены в виде автономных программно-аппаратных блоков, то они устанавливаются в каналы связи, в противном случае — на серверы и рабочие станции пользователей.

6.4.2. Обеспечение конфиденциальности и целостности электронных документов

Информационные атаки нередко предпринимаются для умышленного искажения передаваемых по сети электронных документов пользователей. Для защиты от таких атак могут быть применены средства, базирующиеся на технологии PKI (Public Key Infrastructure). Этой технологией предусмотрено использование асимметричных криптоалгоритмов на уровне самих электронных документов, а не пакетов данных.

Напомним, что асимметричная схема требует наличия двух разных криптографических ключей — открытого и закрытого. Такая схема обладает следующими особенностями:

- ключи могут существовать только в парах открытый ключ/закрытый ключ. При этом одному открытому ключу соответствует только один закрытый ключ;
- значение закрытого ключа невозможно вычислить, имея доступ только к открытому ключу;
- открытый ключ свободно распространяется по общедоступным каналам связи, в то время как закрытый хранится в секрете.

Для безопасного обмена открытыми ключами между пользователями ИС служат цифровые сертификаты. Сертификат представляет собой структуру данных, содержащую открытый ключ владельца сертификата; он подписывается выдающей его службой.

В качестве последней выступает так называемый удостоверяющий центр. Таким образом, выдавая сертификат, удостоверяющий центр гарантирует соответствие открытого ключа субъекта идентифицирующей его информации.

Технология PKI обеспечивает целостность передаваемых в ИС документов посредством механизма электронной цифровой подписи (ЭЦП). ЭЦП — это не что иное, как реквизит документа, позволяющий устанавливать отсутствие искажения содержащейся в документе информации, а также однозначно определять обладателя подписи. Схема алгоритмов формирования и проверки ЭЦП показана на рис. 6.3.

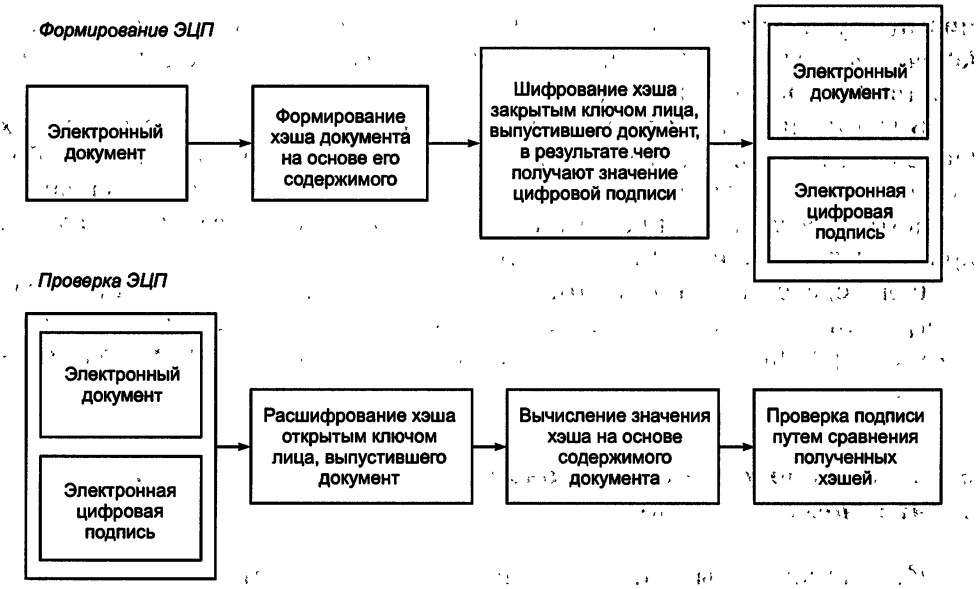


Рис. 6.3. Схема применения электронной цифровой подписи

Формат электронного документа с ЭЦП должен соответствовать международным стандартам PKCS7 и S/MIME.

Криптографические методы, используемые в технологии PKI, также могут быть применены и для обеспечения конфиденциальности передаваемых через корпоративную почтовую систему электронных документов.

В этом случае защита электронных документов осуществляется посредством их шифрования открытыми ключами, содержащимися в сертификатах получателей этих документов. При этом зашифрованный документ должен соответствовать международному стандарту PKCS7. Для расшифровки документов их получатели используют свои закрытые ключи. Процедура работы с защищенным почтовым сообщением показана на рис. 6.4.

Для обеспечения криптографической защиты почтовых сообщений на рабочие станции пользователей нужно устанавливать дополнитель-

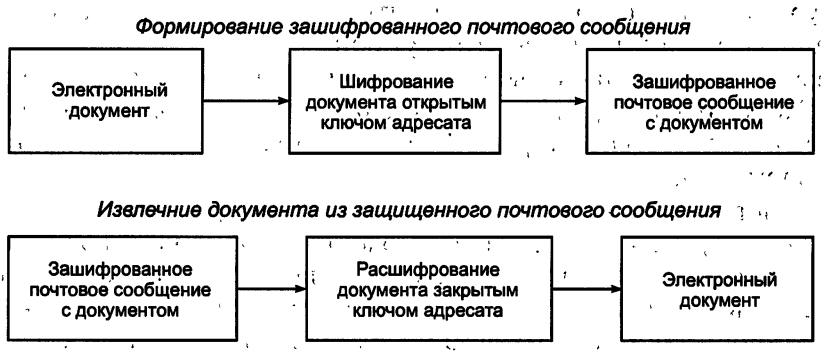


Рис. 6.4. Схема работы с защищенным почтовым сообщением

ные программные средства, реализующие технологию PKI. Эти средства выполняют следующие функции:

- шифрование/расшифровку почтовых сообщений с добавлением/проверкой ЭЦП. При этом средства защиты должны поддерживать отечественные криптоалгоритмы, закрепленные ГОСТ 28147—89 и ГОСТ Р 34.10/11—94;
- блокирование входящих и исходящих почтовых сообщений, не защищенных криптографическими методами;
- ведение архива входящих и исходящих сообщений;
- ведение журнала аудита, в котором регистрируются все криптографические операции, выполненные над входящими и исходящими почтовыми сообщениями.

6.4.3. Обеспечение работоспособности почтовых серверов

Почтовые серверы ИС предприятия тоже могут стать объектами сетевых атак, направленных на нарушение их функционирования. Успешность атак этого типа возможна из-за уязвимостей, которые присутствуют в ПО почтовых серверов. Причинами возникновения таких уязвимостей являются плохое программирование, некорректная конфигурация сетевых почтовых сервисов и пр.

Чтобы защитить почтовые серверы от подобных атак, необходимо использовать средства, способные выполнять функции выявления и устранения уязвимостей, а также обнаружения и блокирования сетевых атак. Для выявления уязвимостей используют специализированные системы анализа защищенности — они сканируют серверы ИС предприятия. В случае обнаружения уязвимости такая система выдает рекомендации по ее устранению.

Выявить и своевременно блокировать сетевые атаки позволяют средства обнаружения вторжений и межсетевые экраны (МЭ). Последние обеспечивают фильтрацию запросов на уровне межсетевого взаимодействия и транспортном уровне стека TCP/IP и блокируют те из них, которые представляют потенциальную угрозу для почтовых серверов. Почтовый сервер подключается к МЭ таким образом, чтобы все запросы, поступающие к нему, проходили через экран.

В дополнение к МЭ для выявления и блокирования сетевых атак на прикладном уровне используются сетевые и серверные датчики обнаружения вторжений. Сетевые датчики устанавливаются перед и позади МЭ и выполняют функции пассивного анализа и выявления атак на почтовый сервер. При этом датчик, установленный перед МЭ, вдобавок позволяет обнаруживать и атаки на сам экран. Для того чтобы не только обнаруживать, но и блокировать сетевые атаки, дополнительно на почтовый сервер необходимо установить датчик обнаружения вторжений уровня хоста, выполняющий функцию блокирования запросов, представляющих опасность для сервера.

6.4.4. Обеспечение антивирусной защиты почтовой системы

Почтовые системы предприятий могут быть использованы злоумышленниками для распространения вредоносных программ — например, таких, как компьютерные вирусы. Типичная вирусная атака на ИС реализуется так: злоумышленник помещает в электронное письмо зараженный вирусом файл и рассылает его пользователям ИС; получение и открытие такого письма на рабочей станции автоматически вызывает запуск инфицированного исполняемого файла и система заражается компьютерным вирусом.

Один из способов антивирусной защиты корпоративной почтовой системы заключается в формировании в рамках ИС криптографически защищенной среды, в которой могут передаваться только зашифрованные и подписанные посредством ЭЦП сообщения. В этом случае любое не защищенное криптографическим методом сообщение рассматривается системой как потенциально опасное и подлежащее блокированию. Реализация такого способа требует установки на все рабочие станции пользователей ИС специализированного ПО. Для усиления защиты рекомендуется установить на рабочие станции антивирусное ПО.

6.4.5. Защита от утечки конфиденциальной информации

Злоумышленники могут использовать почтовую систему ИС предприятия и в качестве канала утечки конфиденциальной информации. В этом случае нарушитель, имея возможность сформировать почтовое сообщение, помещает в него конфиденциальные данные и отправляет его за пределы ИС. При этом для отправки сообщений он может воспользоваться не только корпоративным, но и внешним почтовым сервером.

Эффективная защита от атак этого типа обеспечивается с помощью системы активного мониторинга (CAM) рабочих станций, позволяющей выявлять несанкционированные действия пользователей ИС. Размещаемые на рабочих станциях агенты CAM способны выявлять и блокировать нарушения установленной политики безопасности. В частности, для обеспечения защиты от утечки конфиденциальной информации администратор CAM может ограничить перечень адресатов, которым пользователи ИС отправляют сообщения, а также явно указать IP-адреса SMTP- и POP3-серверов — через них (и только через них!) пользователи имеют право работать с почтовой системой ИС.

Исходя из всего вышесказанного можно сделать очевидный вывод, что для организации эффективной защиты почтовой системы, входящей в состав ИС предприятия, необходимо создание комплексной системы безопасности, базирующейся на рассмотренных средствах. Описание такой системы приводится ниже.

6.4.6. Комплексный подход к защите корпоративной почтовой системы

Рассмотрим пример построения защищенной корпоративной почтовой системы, включающей в себя как почтовые серверы, так и локальных и удаленных пользователей. Локальные пользователи работают с почтовой системой, находясь внутри корпоративной ИС, а удаленные — вне ИС, через сеть Интернет. Взаимодействие между пользователями и серверами осуществляется по протоколам SMTP и POP3. На рис. 6.5 приведена архитектура защищенной системы электронной почты.

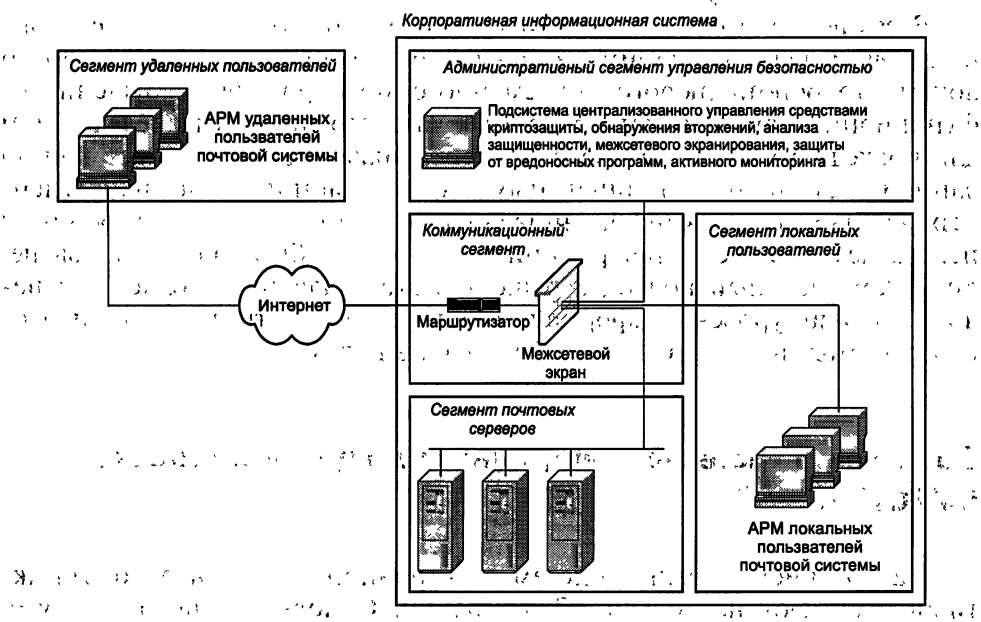


Рис. 6.5. Архитектура защищенной системы электронной почты

Система обеспечения информационной безопасности электронного документооборота предприятия должна включать в себя семь подсистем: межсетевого экранирования, обнаружения вторжений, анализа защищенности, криптографической защиты, активного мониторинга, антивирусной защиты и управления. Все они размещаются в ИС, которая функционально разделяется на следующие сегменты:

- сегмент почтовых серверов, с размещенными в нем SMTP/POP3-серверами ИС. В данном сегменте устанавливаются серверные датчики подсистемы обнаружения вторжений, предназначенной для выявления и блокирования сетевых атак, а также датчики подсистемы антивирусной защиты, позволяющие обнаруживать враждебный код и удалять его из ИС;
- коммуникационный сегмент с коммутаторами и маршрутизаторами, а также с подсистемой межсетевого экранирования и сетевыми датчиками подсистемы обнаружения вторжений;

- административный сегмент управления безопасностью ИС с установленными в нем подсистемой анализа защищенности, позволяющей выполнять функции выявления уязвимостей в ПО ИС, и подсистемой централизованного управления всем комплексом средств защиты;
- сегменты локальных и удаленных пользователей ИС, в которых размещаются антивирусные датчики, специализированное ПО подсистемы криптографической защиты и датчики подсистемы активного мониторинга. Последние обеспечивают защиту от потенциальной утечки конфиденциальной информации через почтовую систему.

В заключение следует отметить, что, поскольку система электронной почты является одним из важнейших компонентов электронного документооборота любого современного предприятия, нарушение ее функционирования может привести к катастрофическим последствиям для последнего. Именно поэтому особое значение приобретает защита данной системы от потенциальных информационных атак, направленных на нарушение конфиденциальности, целостности и доступности передаваемой в ней информации. И, как уже было показано выше, лишь комплексный подход к решению этой задачи позволяет обеспечить высокий уровень информационной безопасности не только почтовой системы, но и всей ИС предприятия в целом.

6.5. Защита системы электронного документооборота DIRECTUM

На российском рынке систем электронного документооборота активно работают несколько ИТ-компаний. Основными потребителями систем электронного документооборота являются крупные российские компании. Сложная, географически распределенная структура этих компаний накладывает определенный отпечаток на требования, предъявляемые к системам корпоративного электронного документооборота.

Наибольшей привлекательностью для крупных компаний обладают системы электронного документооборота, ориентированные на организацию удаленного доступа к ресурсам, т. е. имеющие веб-интерфейс и использующие мощную базу данных. Важным компонентом такой системы документооборота является электронная почта.

Прикладные решения для электронного документооборота, предложенные ИТ-компаниями, представлены в табл. 6.3.

Развитие российских разработок идет в соответствии с потребностью компаний-заказчиков автоматизировать максимальное количество бизнес-процессов и обеспечить единое информационное пространство. Это достигается за счет развития таких характеристик систем, как наличие полноценного хранилища контента, механизмы управления контентом, в том числе обеспечение полноценного процесса делопроиз-

Таблица 6.3. **Прикладные решения для электронного документооборота**

Компания	Продукт	Назначение продукта
Directum	DIRECTUM 4.5	Система электронного документооборота и управления взаимодействием
Электронные Офисные Системы	Дело 8.9	Промышленная система автоматизации делопроизводства и электронного документооборота
Naumen	Naumen DMS 2.0	Автоматизация бизнес-процессов и документооборота в крупных компаниях
Cognitive Technologies	ЕВФРАТ-Документооборот 12.2	Комплексное решение для организации электронного документооборота
Евроменеджмент	Escom.doc 2.0.2	Автоматизация простых и сложных процессов документооборота
UpScale Soft	OPTiMA-WorkFlow 1.19	Система конфиденциального электронного документооборота
ИнтерТраст	OfficeMedia R.5.5 и CompanyMedia R.3.3	Универсальная система электронного документооборота

водства, с возможностью автоматизации специфических бизнес-процессов. Все это должно сочетаться с высокой масштабируемостью.

Система электронного документооборота и управления взаимодействием DIRECTUM 4.5, предлагаемая компанией Directum, удовлетворяет указанные потребности компаний-заказчиков и нацелена на повышение эффективности работы всех сотрудников организации в разных областях их совместной деятельности. Система DIRECTUM соответствует концепции ECM и поддерживает полный жизненный цикл управления документами, при этом традиционное «бумажное» делопроизводство органично вписывается в электронный документооборот [26].

Рассмотрим подробнее функциональные возможности и архитектуру системы DIRECTUM.

6.5.1. Функциональность системы DIRECTUM

Система электронного документооборота DIRECTUM является полноценной ECM-системой (Enterprise Content Management) и поддерживает полный жизненный цикл управления документами, при этом традиционное бумажное делопроизводство органично вписывается в электронный документооборот.

DIRECTUM обеспечивает эффективную организацию и контроль рабочих процессов на основе управления выполнением задач: согласования документов, обработки сложных заказов, подготовки и проведе-

ния совещаний, поддержки цикла продаж и других процессов взаимодействия (рис. 6.6).

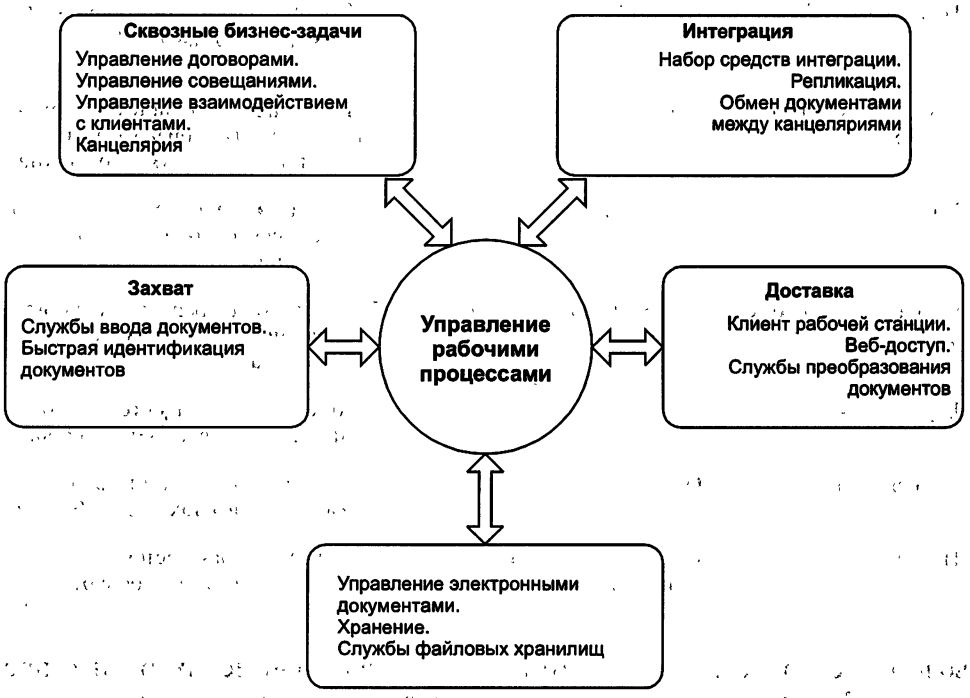


Рис. 6.6. Обобщенная схема реализации рабочих процессов системой DIRECTUM

Решение указанных задач обеспечивают модули системы DIRECTUM:

- *управление электронными документами.* Создание и хранение различных неструктурированных документов (тексты Microsoft Word, таблицы Microsoft Excel, схемы Microsoft Visio, изображения CorelDraw, видео и пр.); расширенная поддержка версий документов и ЭЦП; структурирование документов по папкам; назначение прав доступа на документы; история работы с документами; полнотекстовый и атрибутивный поиск документов;
- *управление рабочими процессами.* Поддержка процессов согласования и обработки документов на всех стадиях жизненного цикла документооборота; выдача электронных заданий и контроль их исполнения; взаимодействие между сотрудниками в ходе бизнес-процессов; поддержка свободных и жестких маршрутов; богатые расширяемые библиотеки блоков для формирования рабочего процесса;
- *управление договорами.* Организация процесса согласования и регистрации договоров и сопутствующих документов, а также оперативной работы с ними (поиск, анализ, редактирование и т. д.);
- *управление совещаниями.* Организация подготовки и проведения совещаний (согласование места и времени, состава участников,

повестки); формирование и рассылка протокола; контроль исполнения решений совещания;

- *канцелярия.* Регистрация бумажных документов в соответствии с требованиями Государственной системы документационного обеспечения управления (ГСДОУ); ведение номенклатуры дел с гибкими правилами нумерации; рассылка и контроль местонахождения бумажных документов; организация обмена электронными документами с ЭЦП с другими организациями;
- *управление взаимодействием с клиентами.* Ведение единой базы организаций и контактных лиц; ведение истории встреч, звонков и переписки с клиентами; сопровождение процесса продаж в соответствии с регламентированными стадиями; планирование маркетинговых мероприятий; анализ эффективности продаж и маркетинговых воздействий.

6.5.2. Архитектура системы DIRECTUM

Система DIRECTUM имеет многоуровневую архитектуру. Архитектура служит гарантом доступности, надежности и безопасности системы, что позволяет системе DIRECTUM охватить всех компьютеризованных сотрудников и повысить эффективность работы организации в целом.

Основными функциональными элементами архитектуры являются (рис. 6.7):

- *СУБД* — хранилище данных и метаданных системы. Одним из важных компонентов системы, хранящихся в СУБД, является прикладная разработка DIRECTUM, которая определяет функциональность предметных модулей системы, заказных, а также разработанных партнерами;
- *управляющие службы DIRECTUM* — службы, обеспечивающие управление системой. Например, служба управления рабочими процессами (WorkFlow) контролирует выполнение задач DIRECTUM, а DIRECTUM Storage Services отвечает за файловые хранилища документов. Все управляющие службы могут быть установлены как на один компьютер, так и на различные — в целях распределения нагрузки;
- *среда исполнения кода (IS-Builder Runtime Environment)*, реализующая интерфейс служб и пользовательских приложений (в том числе сторонней разработки) для доступа к системе. В частности, сервер веб-доступа DIRECTUM использует IS-Builder Runtime Environment для реализации всех функций системы, которые становятся доступны пользователям через веб-браузер;
- *клиенты системы DIRECTUM* — приложения для конечных пользователей, инструментарий разработки, утилиты администрирования системы. Клиентом может быть как Windows-приложение, использующее для доступа к системе IS-Builder Runtime Environment, так и веб-браузер;

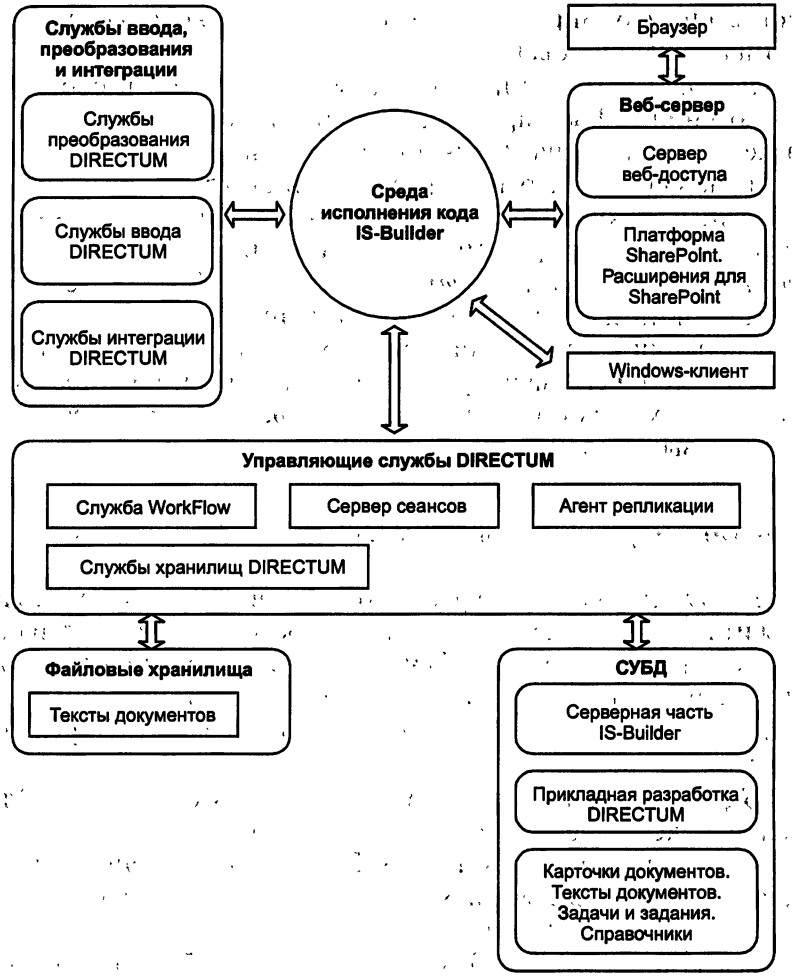


Рис. 6.7. Архитектура системы DIRECTUM

- *файловые хранилища* — архивы больших или редко используемых документов, которые эффективнее держать за пределами СУБД; управляются собственными службами.

Архитектура системы DIRECTUM, являющейся частью информационной инфраструктуры организации, имеет характеристики, важные для любой корпоративной системы:

- *открытость.* Основа системы DIRECTUM — платформа IS-Builder — поддерживает технологии Microsoft COM и .NET. Она содержит готовые инструменты интеграции с корпоративными приложениями, в том числе набор функций для обработки XML-документов. Корпоративные стандарты и открытая структура данных позволяют интегрировать DIRECTUM в информационную инфраструктуру организации;
- *расширение функциональности.* Как правило, в каждой организации выдвигают уникальные требования к построению электронного

документооборота и решению задач взаимодействия. Объектная модель и предметно-ориентированный инструмент разработки IS-Builder позволяют создавать собственные и изменять существующие объекты для решения специфичных задач. Поскольку ядром системы является COM-сервер, управляющие функции системы можно использовать в любых сторонних приложениях;

- *масштабируемость.* Выделение нескольких уровней архитектуры позволяет повышать производительность системы не только посредством наращивания мощности аппаратных средств, но и благодаря распределению служб по различным серверам. Механизм репликации IS-Builder позволяет построить территориально распределенную систему, минимизируя как требования к пропускной способности каналов связи за счет объема передаваемых данных между серверами, так и технические требования к вторичным серверам. Выделение как SQL-серверных, так и файловых хранилищ документов позволяет гибко управлять распределением нагрузки на серверы организации при доступе к документам;
- *надежность.* Архитектура DIRECTUM поддерживает транзакционную модель, которая гарантирует целостность данных системы на протяжении всех стадий их жизненного цикла. Управляемые SQL- и файловые хранилища документов позволяют организовать надежное хранение документов;
- *безопасность.* Для каждого объекта системы может быть задано, какие пользователи или группы имеют право выполнять с ним определенные действия. Конфиденциальные электронные документы и задачи могут быть зашифрованы непосредственно в системе любым CryptoAPI-совместимым криптопровайдером (в том числе сертифицированным ФСБ), что гарантирует защиту даже от лиц, имеющих неограниченный доступ к данным. Протоколирование всех действий пользователя позволяет восстановить историю работы с объектами системы в случае нарушения режима безопасности. Обеспечивается надежная защита от несанкционированного доступа к хранилищам документов всех типов.

Возможности системы DIRECTUM существенно расширяются благодаря следующим компонентам:

- *предметно-ориентированный инструмент разработки IS-Builder.* Модификация и разработка новых карточек электронных документов, справочников, отчетов, блоков типовых маршрутов; встроенный язык программирования ISBL; интеграция с другими системами;
- *службы файловых хранилищ (DIRECTUM Storage Services).* Управление хранением большого объема данных в единой системе; архивное хранение документов; работа с медиа-данными; настройка политик хранения, обеспечивающих автоматическое перемещение данных по хранилищам;
- *сервер веб-доступа.* Работа с электронными документами, задачами и заданиями через веб-браузер;

- *SharePoint* — веб-ориентированная платформа для совместной работы и управления документами, разработанная компанией Майкрософт. Это решение используется для создания корпоративного веб-портала, на котором размещаются совместно используемые документы или специализированные приложения. Данные в SharePoint организованы в виде списков (например, задачи, обсуждения, календари) и библиотек документов. Функциональность SharePoint предоставляется пользователю посредством веб-частей — элементов управления, показывающих списки и позволяющих редактировать их;
- *расширения для SharePoint.* Набор готовых веб-частей и интеграционных механизмов, обеспечивающих доступ к данным DIRECTUM из портала на базе Microsoft SharePoint;
- *сервер репликации.* Создание территориально распределенных систем, обменивающихся данными в офлайновом режиме; иерархическая система вторичных серверов; настраиваемый состав реплицируемых данных;
- *DIRECTUM OverDoc.* Просмотр, редактирование и подписание документов ЭЦП вне системы DIRECTUM для обмена между разными организациями; распространяется бесплатно;
- *технология быстрой идентификации документа DIRECTUM RapID.* Маркировка документа штрих-кодом и быстрый поиск электронного документа по его бумажной копии;
- *службы ввода документов (DIRECTUM Capture Services).* Массовый ввод документов в DIRECTUM с различных источников (сканеры, МФУ, файловая система, факсы, электронная почта и т. д.);
- *службы преобразования документов (DIRECTUM Transformation Services).* Преобразование документов в другие форматы, извлечение из документов полезной информации;
- *набор средств интеграции (DIRECTUM Integration Toolset).* Легкая интеграция с ERP-системами: двусторонняя синхронизация справочников, включение объектов системы в список службы управления рабочими процессами, генерация документов и доступ к ним из ERP-системы.

Архитектура системы DIRECTUM позволяет создавать масштабируемые, надежные и безопасные корпоративные решения для управления документами, бизнес-процессами, совещаниями, договорами и взаимодействием с клиентами.

Адаптация системы DIRECTUM к специфическим нуждам организации и развитие системы вместе с ростом потребностей бизнеса обеспечивается возможностями инструмента разработки IS-Builder, который предлагает развитые средства быстрого и удобного создания новых справочников, карточек электронных документов, сценариев, экранных форм, типовых маршрутов, их отдельных блоков и других компонентов корпоративной системы электронного документооборота.

Интеграция системы DIRECTUM с ERP-системами, корпоративными порталами и другими составными частями ИТ-инфраструктуры ор-

ганизации возможна по различным направлениям благодаря развитым интеграционным возможностям платформы DIRECTUM на базе набора средств интеграции DIRECTUM Integration Toolset и открытой архитектуре.

Территориально распределенная работа крупных организаций поддерживается сервером репликации, который обеспечивает прозрачный для пользователей и разработчика обмен данными — документами, задачами, заданиями, справочниками — между подразделениями организации.

Работа с DIRECTUM через Интернет и в интранете реализована в DIRECTUM по нескольким направлениям. Сервер веб-доступа обеспечивает работу пользователей с документами и задачами DIRECTUM через интерфейс браузера, а расширения DIRECTUM для SharePoint предлагают специализированный интерфейс доступа к данным системы DIRECTUM через корпоративный портал.

Обмен документами между сторонними организациями возможен благодаря специальным механизмам DIRECTUM, позволяющим передавать и контролировать доставку официальной корреспонденции в электронном виде на основе отраслевого формата обмена электронными документами.

Обмен электронными документами между организациями-партнерами, даже в случае отсутствия системы электронного документооборота у любой из сторон, возможен с помощью бесплатной программы DIRECTUM OverDoc на основе специально разработанного формата структурированного электронного документа.

Инструменты администрирования DIRECTUM позволяют управлять всеми задачами администрирования — от регистрации пользователей до создания политик миграции документов между файловыми хранилищами.

В связи с ограниченным объемом книги мы рассмотрим подробнее работу лишь одного из основных модулей системы DIRECTUM — «Управление электронными документами».

6.5.3. Управление электронными документами в системе DIRECTUM

Постоянное увеличение объема накапливаемых в организации документов (приказов, писем, договоров, служебных записок, инструкций и т. д.) приводит к увеличению объема трудно решаемых задач: поиска документов, поддержания их в актуальном состоянии, обеспечения конфиденциальности и сохранности документов и т. д. В результате возникает ситуация информационной недостаточности, управленческие решения принимаются неоперативно, а управленческие затраты на документооборот увеличиваются. Все это негативно сказывается на эффективности работы организации в целом.

Для решения указанных задач в системе DIRECTUM выделен модуль «Управление электронными документами», с помощью которого

все сотрудники организации работают с документами преимущественно в электронном виде. Модуль обеспечивает создание, хранение, поиск документов, изменение различных неструктурированных документов (тексты Microsoft Word, электронные таблицы Microsoft Excel, изображения Visio и CorelDraw, звуки, видео и пр.).

Одно из основных понятий, используемых в системе DIRECTUM, — *электронный документ*. Каждый электронный документ состоит из *текста* — содержимого электронного документа — и *карточки* — формы, содержащей набор атрибутов, описывающих документ (автор, тип документа, дата создания, корреспондент и т. д.), — которые могут быть использованы для поиска и группировки электронных документов. Для организации хранения документов используются *папки*, в которые помещаются *ссылки* на электронные документы и другие папки.

Каждый документ может иметь неограниченное количество *версий*, при этом версии одного и того же документа могут быть в разных форматах (например, DOC и PDF). Для каждого вида документа (договоры, счета и пр.) определяется свой *жизненный цикл*, автоматически изменяющий состояние документа в ходе работы с ним.

Модуль использует возможности файловых хранилищ для организации работы с документами большого объема, а также для создания долговременного архива электронных документов.

Ввод и преобразование документов

Внедрение системы электронного документооборота позволяет значительно сократить объем бумажных документов. Однако полностью исключить бумагу и перейти на электронную документацию невозможно, так как правовые нормы до сих пор требуют наличия бумажной документации, а значительная часть информации поступает в компанию не в электронном виде.

Для облегчения ввода информации с различных носителей в системе DIRECTUM предусмотрены службы ввода документов DIRECTUM Capture Services (рис. 6.8). Службы обеспечивают массовый ввод документов со сканеров, МФУ (сендеров), папок файловых систем, факсов и т. д.

Службы включают в себя специальные сервисы по интеграции с оборудованием и захвату образов документов:

- сервис ввода с потокового сканера;
- сервис ввода с факса;
- сервис ввода из файловой системы;
- сервис извлечения штрих-кода;
- сервис группировки изображений.

DIRECTUM Capture Services также реализует первичную обработку документов, например разделение потока страниц по разным признакам — наличию и типу штрих-кода, белому листу, количеству страниц и т. д.

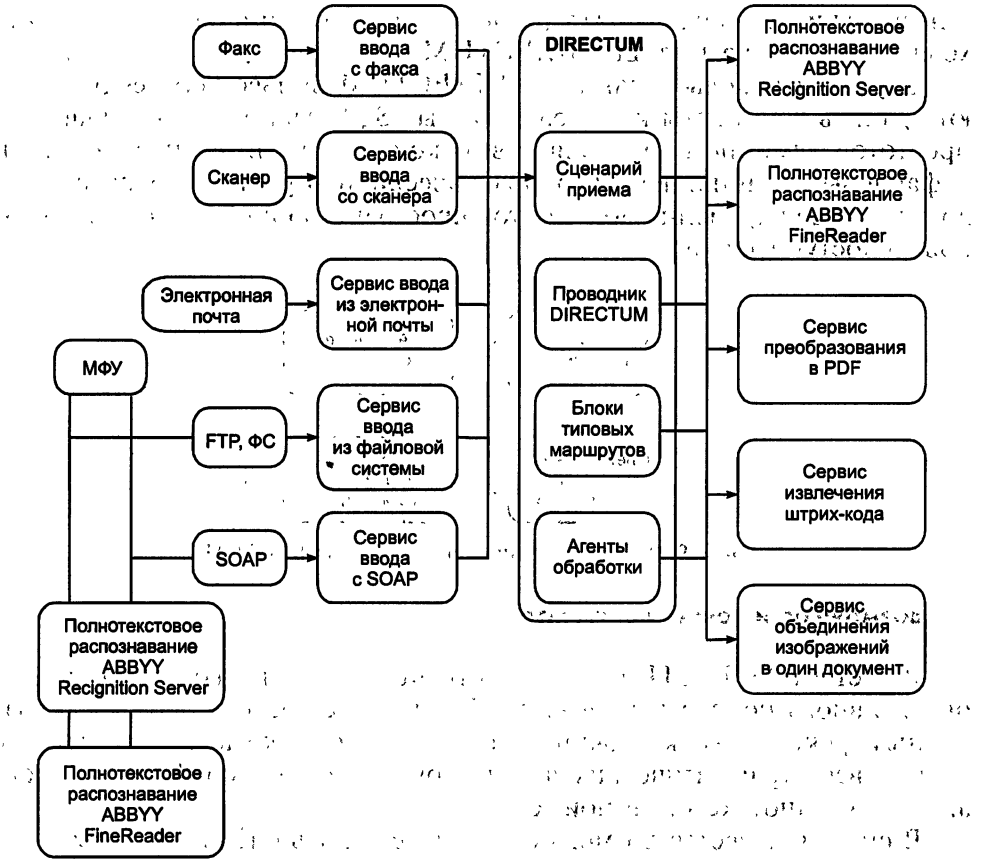


Рис. 6.8. Службы ввода документов в системе DIRECTUM

Дальнейшая обработка занесенных в систему документов может осуществляться службами преобразования документов DIRECTUM Transformation Services, которые переводят документы в другие форматы (в частности, в формат PDF) и извлекают из них необходимую информацию.

Организация хранения документов

Хранение документов в системе DIRECTUM организовано таким образом, чтобы обеспечить удобство работы пользователей и гарантировать сохранность, конфиденциальность и быстрый поиск документов. Размещение всех документов в едином информационном пространстве системы DIRECTUM избавляет каждого пользователя от проблемы поиска документов, созданных другими пользователями в локальных каталогах на своих компьютерах, и от проблемы доступа к таким документам. При этом каждый пользователь системы DIRECTUM может организовать удобную лично ему иерархию папок, куда помещается не сам документ, а ссылка на него. В результате один документ может «лежать»

в нескольких папках, а может не присутствовать ни в одной папке, находясь только в хранилище DIRECTUM.

Службы файловых хранилищ DIRECTUM Storage Services позволяют хранить документы как в базе данных SQL-сервера, отличающегося простотой администрирования и высокой производительностью, так и в файловых хранилищах, что практически неограниченно расширяет доступное для хранения документов пространство и обеспечивает потоковый доступ (рис. 6.9).

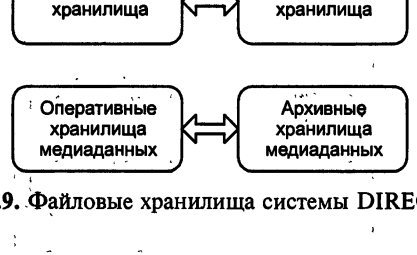


Рис. 6.9. Файловые хранилища системы DIRECTUM

Возможности поиска документов

В системе DIRECTUM предусмотрены различные возможности для оперативного поиска документов. Поиск может осуществляться по заданным реквизитам карточки, а также по содержимому документа с учетом всех грамматических форм слов на основе морфологического анализа (полнотекстовый поиск).

В системе имеется возможность осуществлять специализированный поиск электронных документов, используя:

- предопределенный поиск (например, «Мои последние измененные документы»);
- дополнительный поиск по часто используемым критериям, специально настроенный администраторами;
- возможность задания для любого документа связанных с ним по смыслу или логике документов и перехода от одного связанного документа к другому, включая его собственные связанные документы.

Кроме того, в системе каждый пользователь может создавать папки поиска. Для таких папок определяются критерии поиска, по которым формируется содержимое папки. При этом содержимое папки актуализируется при каждом ее открытии.

Для поиска документов по бумажному аналогу используется технология быстрой идентификации документа DIRECTUM Rapid Document Identification (RapID). Используя маркировку бумажных аналогов документов уникальным штрих-кодом и применяя в дальнейшем сканер штрих-кодов, пользователи могут найти электронный документ в системе оперативно и безошибочно. Штрих-код позволяет однозначно идентифицировать документы и исключить ошибки, вызванные несовпадением электронного и бумажного документов. При сканировании

штрих-кода документ открывается в специальном, удобном пользовательском интерфейсе, облегчающем работу руководителей и делопроизводителей.

Работа с содержимым документа

Система DIRECTUM позволяет использовать любые программы для создания и редактирования электронных документов (Microsoft Word, Microsoft Excel, Microsoft Project, Microsoft Visio, AutoCAD, CorelDraw и др.)

Для оперативного создания однотипных электронных документов используются шаблоны, определяющие начальное содержимое документа, например «Исходящее письмо», «Договор поставки», «Коммерческое предложение» и т. п. При этом в текст документа может автоматически подставляться содержимое полей, заполненных в карточке документа.

Функция импорта документов позволяет легко занести документ в систему из любого файла операционной системы, а также непосредственно со сканера. Документ также может быть занесен в систему из электронного письма благодаря интеграции DIRECTUM с Microsoft Outlook.

Интеграция с Microsoft Word, Microsoft Excel, Microsoft Project, а также с бесплатно распространяемым пакетом офисных приложений OpenOffice.org позволяет непосредственно из приложения отправлять документ на согласование, просматривать историю работы с документом и связанные документы, вставлять штрих-код и сравнивать версии документов.

Жизненный цикл и версии документа

Каждый документ в системе DIRECTUM может иметь неограниченное количество версий. Это позволяет хранить историю изменения содержимого документа (например, в процессе согласования) и избегать работы с устаревшей информацией. При этом версии одного и того же документа могут быть в разных форматах, что облегчает поиск, хранение и доступ к документу и значительно повышает удобство работы пользователей. Например, версии, возникающие в процессе разработки и согласования, могут храниться в удобном для редактирования формате DOC, а окончательная согласованная версия — в неизменяемом формате PDF.

Версия электронного документа отражает актуальность его содержимого. Каждая версия может находиться в одном из состояний: в разработке, действующая, устаревшая. Для визуального представления состояния версии используется особое начертание шрифта. Для каждого вида документа (договоры, счета и пр.) предусматривается свой жизненный цикл, в котором задаются стадии жизненного цикла и правила перехода между ними. Переход между стадиями может осуществляться автоматически. Например, жизненный цикл вида документа «Входящий счет на оплату» включает стадии «Инициализация», «Внутреннее

согласование», «Отказано в оплате», «Оплата», «Оплачен». В процессе работы с документом в модуле «Управление рабочими процессами» стадии будут автоматически меняться, соответственно изменяя состояние документа и его визуальное представление в системе. Управление жизненным циклом документа осуществляется при помощи удобного графического редактора.

Обеспечение конфиденциальности документов

Одной из важнейших функциональных задач системы DIRECTUM является защита информации от несанкционированного доступа. Конфиденциальность документов, хранящихся в системе DIRECTUM, обеспечивается следующими возможностями:

- контролем и настройкой прав доступа на любой объект системы, (полный доступ, изменение, просмотр, полное отсутствие доступа), обеспечивающими защиту от несанкционированного доступа;
- шифрованием электронных документов, позволяющим дополнительно защитить текст электронного документа, в том числе от пользователей со статусом администратора; шифрование может осуществляться как на основе сертификата закрытого ключа пользователя (хранимого в том числе на переносном ключе), так и установкой обычного пароля;
- протоколированием всех действий пользователей, позволяющим быстро восстановить историю работы с документом и фиксировать такие действия над документом, как просмотр, изменение, экспорт копии документа и пр.

Для предотвращения прямого доступа к текстам документов, минуя систему DIRECTUM, реализованы специальные средства защиты, как файловых хранилищ, так и хранилищ на SQL-сервере.

Использование электронной цифровой подписи

Электронная цифровая подпись (ЭЦП) позволяет заменить традиционные печать и подпись, гарантируя авторство и неизменность документа после его подписания. С помощью ЭЦП можно подписать любую версию электронного документа, фиксируя и сохраняя информацию о том, кто и когда поставил подпись.

Система DIRECTUM поддерживает два вида ЭЦП: визирующую и утверждающую. *Визирующая подпись* свидетельствует о том, что подписавший документ ознакомился с ним (завизировал его).

Утверждающая подпись может быть поставлена ограниченным кругом лиц в рамках заданных полномочий и свидетельствует об окончательном утверждении документа. Подпись любого вида, поставленная на версии документа, защищает ее от изменений.

Надежность работы с ЭЦП в системе DIRECTUM обеспечивает использование переносных ключей (USB-ключей, смарт-карт), позволяю-

щих хранить персональный ключ пользователя не на общедоступном компьютере, а на индивидуальном носителе. Для повышения надежности работы с ЭЦП система DIRECTUM может быть интегрирована с различными системами криптозащиты информации, в том числе сертифицированными ФСБ (ФАПСИ), благодаря реализации ЭЦП с использованием Microsoft CryptoAPI.

Организация коллективной работы с документами

При одновременной работе большого количества пользователей в едином информационном пространстве возникает проблема одновременного редактирования одного документа несколькими пользователями. Для решения этой задачи в системе DIRECTUM предусмотрен специальный механизм блокировок. Благодаря ему пользователи могут одновременно редактировать разные версии документа и карточку, а также создавать новые версии, в том числе в различных форматах. При этом остальные пользователи могут просматривать редактируемые версии и карточку документа. Автоматически создаваемые теневые копии документа позволяют вернуться к случайно удаленному или некорректно измененному содержимому документа.

В системе существует возможность получения оповещений об освобождении документа, если при попытке открытия этот документ был уже заблокирован другим пользователем. Это позволяет быстро вернуться к документу сразу после того, как другой пользователь освободит его.

Система DIRECTUM позволяет также работать с отдельными документами в автономном режиме (например, забрать файл домой, поработать, потом возвратить). Для этого существуют возможности экспорта документа из системы и импорта документа в систему, а также возможность блокировки экспортированного документа до тех пор, пока не будет произведен его возврат в систему. Экспорт документа также возможен не только в оригинальный формат, но и в ZIP-архив, в PDF, а также в специально разработанный открытый формат структурированного электронного документа ESD.

ESD-документ содержит все атрибуты карточки и электронные подписи, т. е. сохраняет юридическую значимость документа и может быть использован для взаимодействия со сторонними организациями. Работа с ESD-документом ведется с помощью свободно распространяемой программы DIRECTUM OverDoc.

Таким образом, система DIRECTUM поддерживает полный комплекс работ с электронными документами, обеспечивая:

- соблюдение режима конфиденциальности доступа к документам;
- применение электронной цифровой подписи;
- надежное хранение документов, в том числе в разных форматах;
- реализацию защищенного электронного документооборота между организациями и т. д.

Вопросы для самоконтроля

1. Опишите преимущества электронного документооборота по сравнению с бумажным. Укажите различия между понятиями СЭД и ECM.
2. Охарактеризуйте базовые составляющие системы электронного документооборота.
3. Опишите функциональность подсистемы автоматизации управления рабочими процессами (WorkFlow).
4. Укажите особенности построения и функционирования системы распределенного электронного документооборота.
5. Назовите угрозы информационной безопасности для СЭД и охарактеризуйте источники этих угроз.
6. Какие функции должны быть реализованы средствами защиты информации СЭД?
7. Назовите основные угрозы информационной безопасности баз данных. Укажите методы и средства защиты СУБД.
8. Определите понятие RAID-массива. Поясните особенности применения RAID-массивов в СУБД.
9. Сравните возможности средств защиты СУБД Microsoft Access и Oracle.
10. Охарактеризуйте методы и средства защиты корпоративного почтового документооборота.
11. Опишите функциональные возможности и архитектуру системы электронного документооборота DIRECTUM.
12. Охарактеризуйте приемы и методы защиты, реализованные в системе DIRECTUM.

ЧАСТЬ III

КОМПЛЕКСНАЯ ЗАЩИТА КОРПОРАТИВНЫХ ИС

Корпоративные информационные системы (КИС) становятся сегодня одним из главных инструментов управления бизнесом современной компании. При этом эффективное применение информационных технологий немыслимо без повышенного внимания к вопросам информационной безопасности. Разрушение информационного ресурса, его временная недоступность или несанкционированное использование могут нанести компании значительный материальный ущерб. Без комплексной защиты информации внедрение информационных технологий может оказаться экономически невыгодным в результате значительного ущерба из-за потерь конфиденциальных данных, хранящихся и обрабатываемых в компьютерных сетях.

Глава 7
ПРИНЦИПЫ КОМПЛЕКСНОЙ ЗАЩИТЫ КОРПОРАТИВНОЙ ИНФОРМАЦИИ

При создании системы защиты корпоративной информации необходимо использовать принцип глубоко эшелонированной обороны от внешних и внутренних угроз. Эта стратегия предполагает необходимость создания многоуровневой системы защиты, при которой прорыв одного уровня защиты не означает краха всей системы безопасности. Комплексный подход к построению системы защиты информации позволяет организовать целостную систему защиты от угроз.

7.1. Архитектура корпоративной информационной системы

Информационные системы повышенной сложности, такие как корпоративные информационные системы (КИС), как правило, состоят из нескольких подсистем, решающих конкретные задачи. При построении КИС следует увязывать подсистемы в единый комплекс, придерживаясь ряда основополагающих принципов:

- использования общепринятых стандартов, поддерживаемых основными фирмами-производителями программного обеспечения;
- применения программного обеспечения достаточной производительности, чтобы его не приходилось менять при увеличении мощности и количества используемого оборудования. Это качество называется масштабируемостью программного обеспечения;
- соблюдения принципа многозвенности, означающего, что каждый уровень системы (клиент, веб-сервер, сервер приложений, сервер баз данных) реализует функции, наиболее ему присущие;
- реализации принципа аппаратно-платформенной независимости и системного программного обеспечения;
- осуществления принципа коммуникативности, когда различные уровни системы могут взаимодействовать между собой как по данным, так и по приложениям [7].

В настоящее время наиболее подходящими технологиями для построения КИС являются экстранет и интранет, предусматривающие

специфические решения для приложений архитектуры клиент—сервер, с использованием всего многообразия технологий и протоколов, разработанных для глобальной сети Интернет.

Имеется в виду, в частности, применение:

- в качестве транспортного протокола — TCP/IP;
- встроенных средств защиты и аутентификации;
- веб-технологии в архитектуре клиент—веб-сервер—сервер приложений—сервер баз данных при разработке приложений [7].

Вместе с тем веб-технологии при всех своих значительных преимуществах вносят и новые проблемы, связанные с масштабируемостью, управлением сеансами и состоянием сети, ее защитой и возможными изменениями стандартов.

Большие нагрузки от пользователей требуют высокоэффективной архитектуры аппаратной и программной платформы, которая должна допускать масштабируемость ресурсов.

Управление ресурсами и разграничение доступа, как правило, ориентированы на отдельный веб-сервер и не охватывают все множество информационных ресурсов корпорации.

Становятся первостепенными проблемы защиты, когда компании делают внутренние базы данных доступными для внешних пользователей. Установление подлинности пользователей и безопасность передачи данных превращается в большую проблему в среде Всемирной сети из-за большого количества потенциально анонимных пользователей.

Что касается стандартов, то веб-технологии все еще изменяются и стандарты до сих пор не сформировались. Например, сейчас происходит расширение HTML языком описания веб-документов XML.

Важнейшими вопросами при реализации КИС на базе технологий Интернет/интранет являются организация защиты информации, централизованного управления информационными ресурсами, разграничение доступа к ресурсам. Особенно это важно для доступа пользователей из внешних сетей к ресурсам КИС, это так называемая экстранет-технология.

Общепринятым подходом к решению вопросов защиты является использование в корпоративной сети, имеющей выход в публичную сеть Интернет, следующей стратегии управления доступом между двумя сетями:

- весь трафик, как из внутренней сети во внешний мир, так и наоборот, должен контролироваться корпоративной системой;
- через систему может пройти только авторизованный трафик, который определяется стратегией защиты.

Межсетевой экран — это механизм, используемый для защиты доверенной сети (внутренняя сеть организации) от сети, не имеющей доверия, например Интернет.

Несмотря на то что большинство МЭ в настоящее время развернуто между Интернетом и внутренними сетями (интранет), имеет смысл использовать их в любой сети, базирующейся на интернет-технологии, скажем, в распределенной сети предприятия.

Перечисленные принципы построения учтены в структурной схеме корпоративной информационной системы, представленной на рис. 7.1. В этой структурной схеме можно выделить такие виды управления, как:

- централизованное управление всей системой предприятия;
- управление подразделениями, приложениями и серверами;
- управление всей сетью;
- управление конечными пользователями [7].

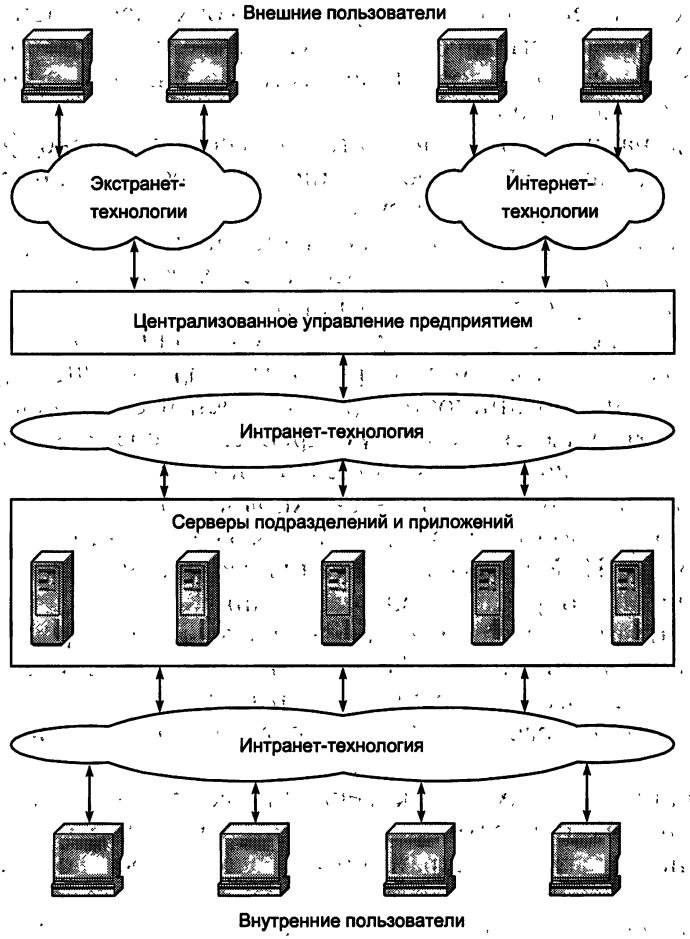


Рис. 7.1. Структурная схема корпоративной информационной системы

Эти четыре уровня управления КИС могут служить объектами угроз для информационной безопасности предприятия.

Соответственно система информационной безопасности КИС должна включать в себя защиту:

- централизованного управления;
- приложений и соответствующих серверов;
- сети;
- конечных пользователей.

Наличие большого числа информационных и вычислительных ресурсов (баз данных и приложений), используемых на предприятии и функционирующих на различных аппаратных и программных платформах, делает актуальной задачу создания и внедрения системы санкционированного доступа к единому информационному пространству предприятия.

Осуществление подобного санкционированного доступа возможно при условии:

- обеспечения соответствующего единого механизма;
- создания единой политики безопасности и защиты информации;
- централизованного и непрерывного контроля за использованием ресурсов и управлением ими.

При этом обязательно должно быть учтено наличие большого числа наследуемых приложений, исторически используемых на том или ином предприятии.

Возможная схема санкционированного доступа к информационным ресурсам предприятия представлена на рис. 7.2.

На этой схеме представлена многозвенная архитектура, состоящая из:

- клиентского уровня — терминальных компьютеров пользователей под управлением ОС MS Windows NT/2000/XP/Vista, использующих один из широко распространенных браузеров: Microsoft Internet Explorer или Netscape Navigator;

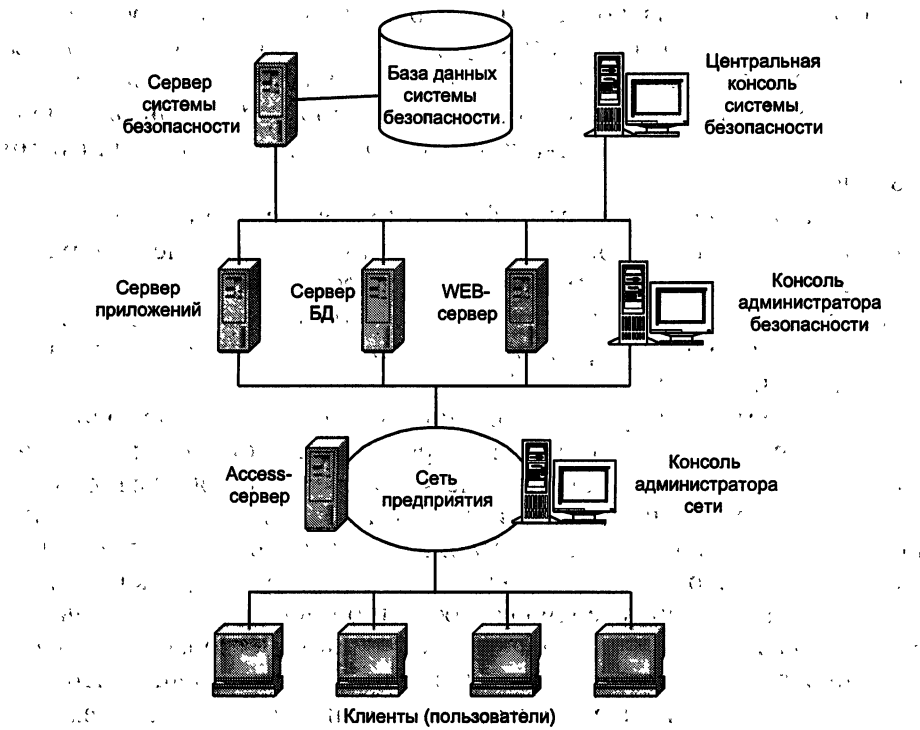


Рис. 7.2. Структурная схема санкционированного доступа к информационным ресурсам предприятия

- уровня серверов доступа (Access Server) — специализированных серверов приложений, реализующих функции аутентификации пользователей, управления правами доступа к ресурсам ИИСУП (распределенный каталог), контроля и протоколирования сеансов доступа к информационным и вычислительным ресурсам ИИСУП;
- уровня серверов приложений — масштабируемой структуры серверов, обеспечивающих унифицированные средства представления информации и функционирования подсистем ИИСУП;
- уровня серверов баз данных;
- уровня веб-серверов.

7.2. Структура системы защиты информации в корпоративной информационной системе

Одной из существенных особенностей КИС является реализация в ней принципа централизованного управления, благодаря чему возможно выполнение таких важных функций, как:

- авторизация и управление распределенной информацией в масштабах всего предприятия;
- возможность централизованной аутентификации и управление контролем доступа ко всем веб-серверам вне зависимости от их платформ (централизованное управление веб-пространством за счет связи веб-серверов в одно логическое веб-пространство);
- управление доступом к персональной информации пользователей;
- централизованное кросс-платформенное управление учетными записями пользователей;
- управление цифровыми сертификатами для электронного бизнеса;
- централизованное кросс-платформенное управление доступом пользователей к информационным ресурсам;
- управление рисками на предприятии, позволяющее системным администраторам контролировать все несанкционированные вторжения на предприятие [7, 58].

Предприниматели постоянно сталкиваются с увеличивающимися рисками от вирусных атак, несанкционированного доступа, а также атак по блокированию программно-технического обеспечения предприятия. Противостоять всем внутренним и внешним (из Интернета) угрозам можно лишь с помощью соответствующей эффективной защиты предприятия. Лучшей ее разновидностью является управление рисками предприятия, когда к его менеджерам своевременно и в необходимых объемах поступает из различных контрольных точек системы безопасности предприятия информация, необходимая для принятия управляющих мер.

Управление рисками предприятия обеспечивается с использованием централизованного пульта (консоли) безопасности предприятия. С его помощью фиксируются, контролируются и устраняются аварийные со-

бытия во всем предприятии. Этот пульт позволяет осуществлять управление угрозами и уязвимостью по всему предприятию, а также гарантировать доступ к сетям, системам, приложениям и рабочим столам, совместимый с политикой защиты предприятия [4].

Управляя рисками предприятия, системные администраторы могут:

- точно идентифицировать различные типы угроз и нападений, используя современную технику корреляций, что очень важно для быстрого ответа по защите предприятия;
- обеспечивать средствами поддержки принятие решений, позволяющих организациям осуществлять профилактические меры по сокращению деловых рисков. Располагая подобными средствами, администраторы по безопасности могут точно определять уязвимые «горячие точки» (hotspots) и осуществлять корректирующие действия, модернизирующие их политику защиты;
- быстро принимать решения по защите от атак по блокированию программно-технического обеспечения, от вирусов или несанкционированного доступа. Меры, предлагаемые в таких случаях, включают в себя нередко реконфигурирование межсетевых экранов, аннулирующее учетные записи пользователя на серверах и удаляющее вирусы с персональных компьютеров.

Управление рисками предприятия вполне согласуется с идеологией неоднородной технологии безопасности разнообразных компьютерных программ. В итоге формируется всестороннее управление информационной безопасностью предприятия.

Подобный принцип управления безопасностью предприятия уже существует и представляет собой открытую, базирующуюся на стандартах, кросс-платформенную систему, позволяющую эффективно бороться с вторжениями и безопасно управлять уязвимостью в сетях, хостах, операционных системах, приложениях, серверах и настольных компьютерах.

В этом случае структурная схема системы защиты информации КИС может быть представлена в виде, показанном на рис. 7.3, где слева указаны уровни защиты информации КИС [58].

Функции уровней защиты могут быть сформулированы следующим образом.

Централизованное управление рисками и администрирование системы безопасности:

- централизованное администрирование;
- административный контроль полномочий главным администратором;
- делегирование части полномочий младшим администраторам отдельных ресурсов;
- управление событиями;
- принятие решений по управлению рисками;
- связь с централизованной консолью управления предприятием;
- долговременное хранение статистики тревог и вторжений;

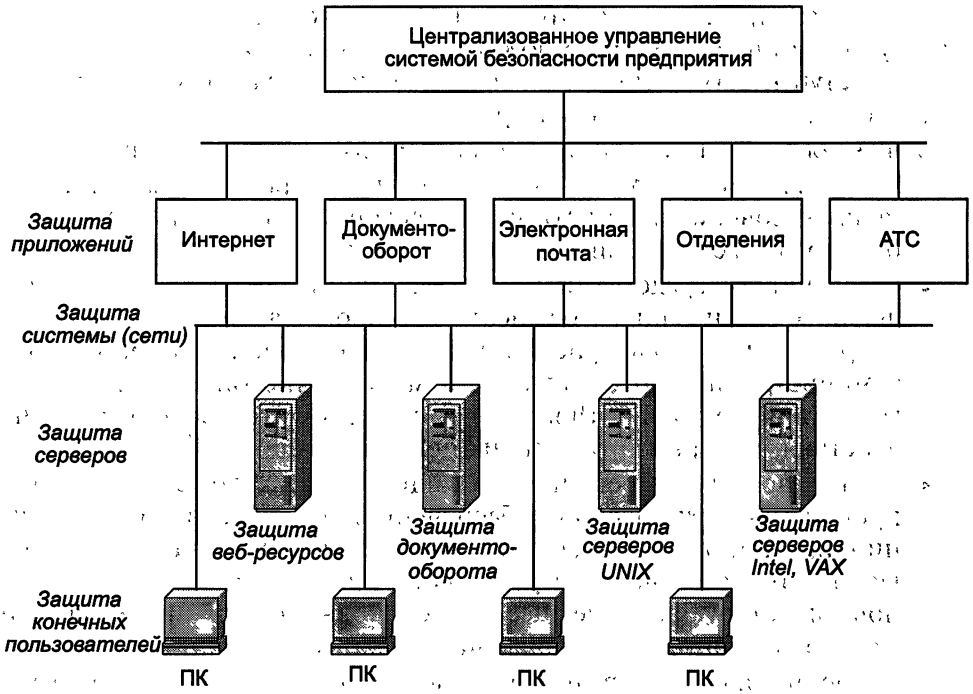


Рис. 7.3. Структурная схема системы защиты информации корпоративной информационной системы

- управление атрибутами пользователей (учетными записями) и обслуживание пользователей в распределенных сетях;
- осуществление централизованной аутентификации и управления контролем доступа ко всем веб-серверам, вне зависимости от их платформ;
- обеспечение консолью центрального управления службой безопасности:
  - управления пользователями: группами и ролями в полной сети предприятия;
  - управления директориями;
  - управления пользовательскими привилегиями;
  - делегирования части административных полномочий младшим администраторам;
  - управления набором ресурсов и распределения администрирования между младшими администраторами.

При этом сама консоль должна позволять отделять управление разработкой политики безопасности от ее реализации.

Защита управления приложениями:

- защита доступа к ресурсам приложений;
- установление и контроль связи учетных записей пользователей с различными типами ресурсов (файлами, директориями, принтерами, приложениями и др.);

- возможность делегирования управления доступом к ресурсам младшим администраторам при высокой степени контроля;
- установление и контроль групповых подсоединений пользователей к ресурсам;
- использование общего административного интерфейса доступа пользователя к ресурсам системы;
- возможность администрирования доступа к ресурсам на правилах, устанавливаемых ролями;
- запрещение неправомочного доступа к информационным ресурсам и критическим сервисам;
- управление аудитом.

Защита системы сетей:

- защита внутрисетевого обмена (локальные вычислительные сети, интранет);
- защита межсетевого обмена (глобальные вычислительные сети, экстранет);
- защита обмена через Интернет;
- осуществление стыковочных узлов, репликация доступа к ресурсам;
- осуществление поддержки любых соединений (back-end), веб-серверов и поддержки соединений с ресурсами;
- осуществление распределения нагрузки для улучшения производительности и восстановления после сбоев.

Защита конечных пользователей:

- установление соответствия имени и пароля;
- управление доступом с помощью списков контроля за пользователями, а также соответствующих правил обращения пользователей с информацией;
- сертификация открытых ключей PKI;
- поддержка статических и динамических ролей (например, доступ для чтения/записи, доступ только для чтения);
- контроль попыток доступа к ресурсам и регистрация (обнаружение угрозы безопасности);
- контроль соблюдения требований политики секретности.

7.3. Комплексный подход к обеспечению информационной безопасности КИС

При разработке архитектуры комплексной системы защиты информации (КСЗИ) необходимо учитывать следующие общие требования:

- информационная безопасность (ИБ) должна быть обеспечена на всех уровнях информационной системы: на организационно-управленческом, технологическом и техническом;

- ИБ должна быть обеспечена на всех стадиях жизненного цикла информационных систем;
- архитектура КСЗИ должна иметь распределенную и многоуровневую структуру, соответствующую структуре информационной системы;
- решения, образующие КСЗИ, должны выбираться с учетом масштабируемости и модульного принципа построения, обеспечивающих наращивание и модернизацию подсистем по мере изменения требований к обеспечению ИБ, возникновения новых угроз, создания новых средств защиты и их модернизации;
- внедрение мер безопасности должно осуществляться в рамках всей инфраструктуры (а не только на критичных ресурсах);
- КСЗИ должна охватывать все этапы обработки информации (создание, сбор, обработку, накопление, хранение, поиск, распространение и использование) и не накладывать жестких ограничений на используемые технологии построения информационных систем;
- КСЗИ должна быть интегрирована со встроенными средствами защиты информации прикладных систем, операционных систем и информационных сервисов.

Комплексная система защиты информации основана на совместном применении следующих мер и средств защиты:

- централизованное управление компонентами КСЗИ и мониторинг сетевой активности;
- использование пакетных фильтров и межсетевого экранирования уровня приложений для разграничения доступа пользователей к ресурсам Интернета и защиты внутренних ресурсов КИС от НСД из Интернета;
- применение разрешительного порядка предоставления пользователям привилегий доступа к ресурсам Интернета;
- обнаружение вторжений на сетевом и прикладном уровнях с соответствующей динамической реакцией на эти атаки, например, путем автоматического переконфигурирования межсетевых экранов и обрыва межсетевых соединений;
- обеспечение антивирусной проверки и удаления вирусов в проходящем через Интернет трафике электронной почты, FTP- и HTTP-трафике;
- гибкая организация демилитаризованных зон и возможности дополнительной защиты критических демилитаризованных зон;
- обеспечение отказоустойчивости и надежности корпоративной сети благодаря:
  - дублированию каналов доступа в Интернет и каналов КИС;
  - разнесению точек выхода из Интернета по различным траекториям;
  - использованию протоколов динамического изменения топологии сети, прозрачному для пользователей;
  - дублированию средств управления КСЗИ;

- эшелонирование защиты:
  - — последовательное размещение пакетных фильтров и межсетевых экранов уровня приложений, использование дополнительных межсетевых экранов для защиты критичных ресурсов;
  - — многоуровневое размещение средств обнаружения вторжений для контроля несанкционированной активности как перед межсетевыми экранами, так и за ними, а также обнаружение атак на межсетевые экраны изнутри КИС;
- централизованный аудит и формирование отчетов о сетевой активности и несанкционированных действиях;
- обеспечение целостности ресурсов КСЗИ и управляющего трафика КСЗИ с помощью штатных средств компонентов КСЗИ;
- обеспечение централизованного контроля за уязвимостью компонентов подсистем защиты.

Комплексная система защиты информации представляет собой целостный и достаточный набор средств защиты от актуальных угроз ИБ, который интегрируется в защищаемую информационную систему [7, 98].

Общая структура комплексной системы защиты информации КИС показана на рис. 7.4.

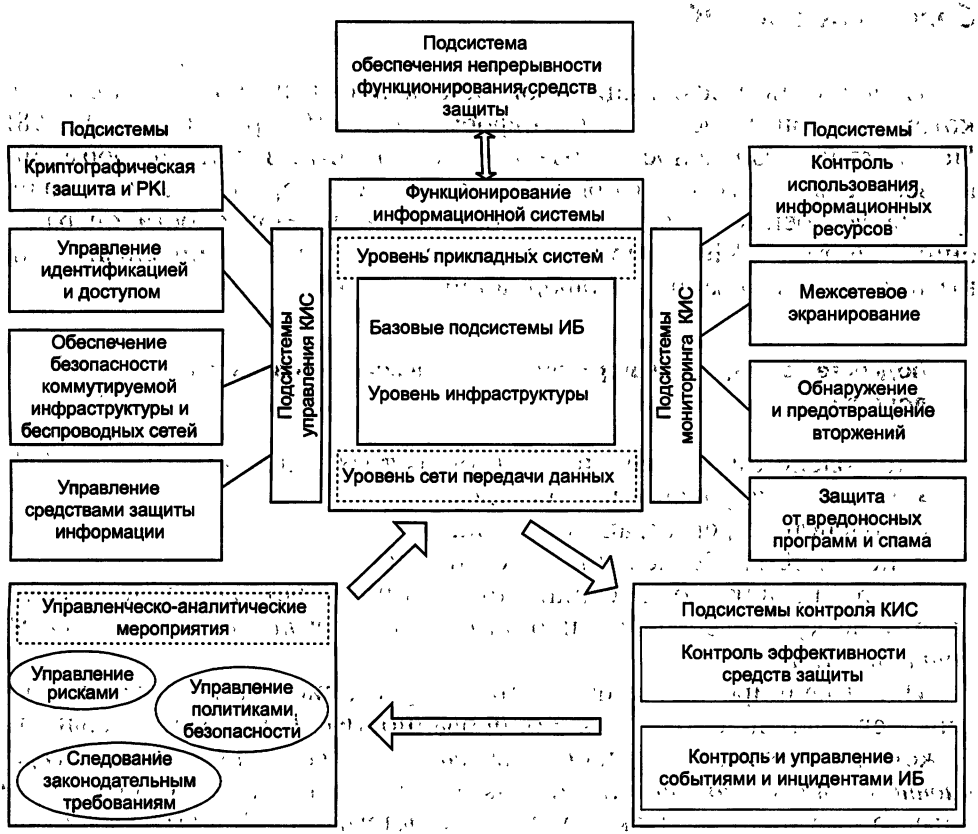


Рис. 7.4. Общая структура комплексной системы защиты информации КИС

В состав КСЗИ обычно входят следующие подсистемы информационной безопасности:

- криптографическая защита и PKI;
- управление идентификацией и доступом;
- обеспечение безопасности коммутируемой инфраструктуры и беспроводных сетей;
- управление средствами защиты информации;
- контроль использования информационных ресурсов;
- межсетевое экранирование;
- обнаружение и предотвращение вторжений;
- защита от вредоносного кода и нежелательной корреспонденции;
- контроль эффективности защиты информации;
- мониторинг и управление инцидентами ИБ;
- обеспечение непрерывности функционирования средств защиты.

Ниже приводится краткая характеристика подсистем информационной безопасности КИС. Наиболее важные технологии защиты корпоративной информации подробно рассмотрены в последующих главах.

7.4. Подсистемы информационной безопасности КИС

Подсистемы информационной безопасности являются основой, на которой строится вся защита информации КИС организации [7, 98]. Подсистемы безопасности позволяют обеспечить защиту информации на всех компонентах информационной системы организации и реализуются встроенными функциями обеспечения безопасности операционных систем, СУБД и прикладных систем, а также специализированными средствами защиты информации.

Подсистема защиты информации от несанкционированного доступа

Эта подсистема состоит из следующих трех подсистем:

- подсистема управления доступом;
- подсистема регистрации и учета;
- подсистема обеспечения целостности.

Система защиты от несанкционированного доступа должна обеспечивать четкую идентификацию *субъекта доступа*, *объекта доступа*, *типа доступа*.

Идентифицировав все параметры запроса, система производит проверку его легальности (санкционированности). Проверка легальности может производиться как на основе *матрицы доступа* (системы *дискреционного управления доступом*), так и на основе меток безопасности объекта и уровня допуска субъекта (системы *мандатного управления доступом*).

Существуют как узкоспециализированные системы защиты информации от несанкционированного доступа (НСД), так и решения, покрывающие все функции системы защиты информации [98].

Для того чтобы система защиты информации от НСД выполняла свои функции в полном объеме, необходима реализация дополнительных функциональных возможностей — регистрации и учета (аудита) событий в системе и обеспечения целостности защищаемой системы.

Функция регистрации и учета предназначена для фиксирования обращений к защищаемым ресурсам, что позволяет позже расследовать инциденты, связанные с утечкой или утратой информации с ограниченным доступом. При этом необходимо учесть, что юридическую силу будет иметь только журнал сертифицированной системы.

Последняя важная задача защиты информации от НСД — это контроль и обеспечение целостности системы. В случае если программные или аппаратные компоненты системы подвергались модификациям, правильность выполнения основной функции системы может быть поставлена под сомнение, поэтому необходимо, чтобы перед стартом компоненты системы сравнивались с эталоном и в случае обнаружения расхождений поступало оповещение о несанкционированной модификации системы и дальнейшая работа системы блокировалась.

Подсистема криптографической защиты

Криптографическая защита данных обеспечивает безопасную передачу данных, а также их хранение. Криптографические методы защиты информации могут применяться на любом уровне взаимодействия информационных систем. Использование криптографических протоколов позволяет придать юридическую значимость процессам обработки электронных документов. Важным компонентом подсистемы криптографической защиты является инфраструктура управления открытыми ключами PKI.

Инфраструктура управления открытыми ключами PKI предназначена для обеспечения защиты и организации безопасного обмена информацией в публичных (Интернет, экстранет) и частных (интранет) сетях за счет использования средств шифрования с открытыми ключами и механизма электронной цифровой подписи. Внедрение инфраструктуры открытых ключей на предприятии позволяет установить доверительные отношения между внутренними, а также внешними пользователями, обеспечить защиту приложений. Инфраструктура управления открытыми ключами и ее компоненты являются основой для создания комплексной системы обеспечения безопасности организации.

Широкое применение криптографических методов защиты информации делает подсистему криптографической защиты наиболее востребованной на рынке в настоящее время, однако данная подсистема не может в одиночку обеспечить комплексную защиту информации предприятия.

Подсистема управления идентификацией и доступом

С ростом числа пользователей информационной системы и числа прикладных систем и сервисов, к которым они должны получать доступ, увеличиваются затраты на администрирование учетных записей пользователей и управление правами доступа к системам и сервисам. Подсистема управления идентификацией и доступом предназначена для повышения безопасности корпоративных приложений и сервисов и снижения затрат на администрирование пользователей в разнородных приложениях и операционных системах.

Подсистема управления идентификацией и доступом строится на основе:

- служб каталогов;
- систем централизованного управления учетными записями и правами доступа;
- средств однократной аутентификации;
- средств двухфакторной аутентификации.

При создании учетной записи пользователя в центральной системе (служба каталога, кадровая система и т. п.) подсистема управления идентификацией и доступом производит автоматическую трансформацию записи в идентификационные записи в целевых системах согласно политикам управления. Такой подход позволяет реализовать модель ролевого управления пользователями, которые автоматически получают необходимые им права на ресурсы в соответствии с должностными обязанностями, определенными через включение их в соответствующие ролевые группы. Альтернативой системе централизованного управления учетными записями и правами доступа выступают системы однократной аутентификации (Single Sign-On).

Использование подсистемы управления идентификацией и доступом позволяет автоматизировать процессы, связанные с созданием, администрированием, удалением учетных записей, предоставлением доступа к ресурсам и управлением правами в разнородных операционных системах, службах каталогов и приложениях.

Подсистема обеспечения безопасности коммутируемой инфраструктуры и беспроводных сетей

Подсистема обеспечения безопасности коммутируемой инфраструктуры и беспроводных сетей основывается на применении технологий контроля и защиты сетевого доступа NAC, 802.1x, VLAN.

Технология трансляции сетевых адресов, NAC (Network Address Translation) позволяет контролировать и проверять на соответствие политике информационной безопасности любой компьютер, подключающийся к корпоративной сети, стационарный или мобильный компьютер, получающий доступ через локальную или глобальную сеть, через

проводное или беспроводное подключение, выделенное или коммутируемое соединение.

Проверка подлинности IEEE 802.1x представляет собой механизм контроля доступа на основе портов, который можно настроить на выполнение взаимной проверки подлинности между клиентами и сетью. После реализации такой настройки любое устройство, которому не удалось пройти проверку подлинности, не сможет участвовать ни в каком взаимодействии с выбранной сетью. Данная технология позволяет отказаться от применения статических ключей шифрования WEP (Wireless Equivalent Privacy).

Помимо генерации и распределения динамических ключей шифрования, стандартом IEEE 802.1x предусмотрены регулярное изменение сеансовых ключей и мониторинг сетевого доступа (с целью учета использования сетевых ресурсов). По данному стандарту управление доступом осуществляется на основе идентификаторов (user name) и паролей пользователей или их цифровых сертификатов. Средства IEEE 802.1x совместимы с существующими системами аутентификации.

Подсистема управления средствами защиты информации

Современные корпоративные информационные системы, как правило, имеют значительную географическую протяженность, насчитывают множество единиц техники и программного обеспечения. Кроме того, требования бизнеса к надежности и безопасности корпоративных информационных систем приводят к росту степени интеграции подсистем друг с другом и усложнению конфигураций отдельных систем.

Чтобы группа администраторов была способна справиться с задачей эффективного управления информационной системой, необходимо применять решения, которые позволяют:

- осуществлять централизованное управление всеми программными и техническими средствами;
- автоматически распространять обновления программного обеспечения, а также дополнительные программные средства на рабочие станции и серверы;
- создавать типовые конфигурации для быстрого развертывания на новых единицах техники;
- создать централизованную базу учетных записей для всех активных сетевых устройств, рабочих станций и серверов.

Регулярное обновление программных средств корпоративной информационной системы позволяет избежать угрозы эксплуатации злоумышленниками известных уязвимостей программного обеспечения.

Централизованное управление конфигурацией рабочих станций, серверов, активного сетевого оборудования позволяет существенно сократить затраты на обеспечение актуальной конфигурации оборудования информационной системы предприятия. Системы централизованного управления конфигурацией непосредственно зависят от систем

централизованного управления учетными записями и правами доступа, а также систем администрирования доступа к сетевому оборудованию.

Подсистема контроля использования информационных ресурсов

Подсистема контроля использования информационных ресурсов предназначена для комплексного контроля электронных информационных потоков в организации. Подсистема разделяется на подсистему контроля циркуляции конфиденциальной информации и подсистемы контроля использования сотрудниками организации сервисов электронной почты и интернет-ресурсов.

Средства контроля использования интернет-ресурсов и электронной почты предназначены для проверки передаваемых и принимаемых данных на соответствие тем или иным условиям информационного обмена и выполнения соответствующих действий по итогам проверки для предотвращения утечки конфиденциальной информации организации.

Использование систем контроля использования информационных ресурсов необходимо для снижения следующих рисков:

- воздействия вредоносного ПО (вирусов, червей, троянских программ);
- компьютерных атак и скрытого проникновения в корпоративную сеть;
- случайной или умышленно организованной утечки конфиденциальной информации;
- бесконтрольного доступа в Интернет, приводящего к снижению производительности труда в организации и снижению пропускной способности корпоративной сети и каналов связи;
- получения нежелательной корреспонденции (спама).

Системы контроля использования электронной почты предназначены для реализации корпоративной политики использования электронной почты путем контроля и архивации электронных отправлений. Все сообщения электронной почты проверяются системой на соответствие положениям политики использования электронной почты, система реагирует на нарушения этой политики согласно заданным правилам.

Системы контроля циркуляции конфиденциальной информации являются мощным классом систем, который предназначен для контроля и управления конфиденциальной информацией на всем ее жизненном цикле и включают в себя функциональность систем контроля доступа использования интернет-ресурсов и электронной почты.

Подсистема межсетевого экранирования

Сеть передачи данных является неотъемлемой частью любой организации, представляя собой платформу для функционирования сервисов и приложений корпоративной информационной системы. В то же время она может являться источником ряда инцидентов информационной

безопасности, связанных с нарушением конфиденциальности, целостности и доступности информации, хранящейся и обрабатываемой на сетевых информационных ресурсах. Данные инциденты информационной безопасности могут быть связаны с действиями как внутренних, или внешних злоумышленников, так и вредоносного программного кода.

Подсистема межсетевого экранирования обеспечивает защиту корпоративной сети передачи данных от внешних сетевых атак, а также защиту критичных внутренних сегментов сети, например сегмента администрирования или серверного сегмента, от действий внутреннего злоумышленника.

Межсетевые экраны могут представлять собой программно-аппаратные комплексы, функционирующие под управлением специально разработанной операционной системы, а также могут являться программными решениями, предназначенными для работы на разнообразных платформах под управлением таких операционных систем, как Windows или Solaris. Системные межсетевые экраны, предназначенные для защиты отдельных рабочих мест или серверов, предоставляют широкие возможности по защите корпоративной информационной системы, позволяя гибко реализовывать корпоративную политику безопасности.

Для защиты корпоративной сети от внешних угроз межсетевые экраны устанавливаются на границе сети, представляя собой первый рубеж защиты периметра корпоративной информационной системы.

Средства межсетевого экранирования в составе корпоративной информационной системы могут работать совместно с рядом подсистем обеспечения ИБ.

Интеграция с подсистемами управления и мониторинга позволяет реализовать централизованный контроль функционирования межсетевых экранов и принимать своевременные меры по предотвращению и минимизации последствий инцидентов ИБ.

Интеграция межсетевых экранов с подсистемами обнаружения и предотвращения вторжений дает возможность совместить функции безопасности в одном устройстве и организовать единый интерфейс управления.

Подсистема обнаружения и предотвращения вторжений

Обнаружение вторжений — это процесс мониторинга событий, происходящих в информационной системе, и их анализа на наличие признаков, указывающих на попытки вторжения: нарушения конфиденциальности, целостности, доступности информации или политики информационной безопасности. *Предотвращение вторжений* — процесс блокировки выявленных вторжений.

Эта подсистема обеспечивает:

- предотвращение вторжений системного уровня;
- предотвращение вторжений сетевого уровня;
- защиту от DDoS-атак.

Атаки DDoS (Распределенный отказ в обслуживании — Distributed Denial of Service) входят в число наиболее опасных по последствиям классов компьютерных атак, направленных на нарушение доступности информационных ресурсов.

Средства подсистемы обнаружения и предотвращения вторжений автоматизируют данные процессы и необходимы в организации любого уровня, чтобы предотвратить ущерб и потери, к которым могут привести вторжения.

Подсистема защиты от вредоносных программ и спама

Подсистема защиты от вредоносных программ и нежелательной корреспонденции (спама) включает в себя:

- антивирусную защиту серверов и рабочих станций;
- антивирусную защиту сообщений электронной почты;
- потоковую антивирусную фильтрацию;
- защиту от нежелательной корреспонденции.

Средства антивирусной защиты должны обеспечивать защиту от вредоносных программ во всех возможных точках их проникновения:

- защиту серверов и рабочих станций пользователей и администраторов;
- защиту почтовых систем;
- защиту шлюзов входа/выхода во внешнюю сеть.

Использование средств антивирусной защиты позволяет предотвратить ущерб из-за уничтожения, искажения ценной информации или нарушения работы средств вычислительной техники.

Подсистема защиты от вредоносных программ интегрируется со следующими подсистемами:

- с подсистемой обеспечения безопасности коммутируемой инфраструктуры и беспроводных сетей для обеспечения блокировки зараженных узлов;
- с подсистемой межсетевого экранирования с целью перенаправления потенциально опасного трафика для антивирусной проверки;
- с подсистемой обеспечения непрерывности функционирования средств защиты с целью резервного копирования конфигураций средств антивирусной защиты и антивирусных баз;
- с подсистемой мониторинга и управления инцидентами для оперативного анализа случаев вирусного заражения, обработки зараженных объектов и оповещения об этом ответственных лиц.

Подсистема контроля эффективности защиты информации

Данная подсистема позволяет автоматизировать процесс контроля эффективности защиты информации:

- анализ уязвимостей сетевой и системной инфраструктуры — деятельность по выявлению уязвимостей в программно-аппаратном

обеспечении на основе всесторонних или выборочных тестов сетевых сервисов, операционных систем, прикладного программного обеспечения, маршрутизаторов, межсетевых экранов и т. п.;

- анализ уязвимостей СУБД или веб-приложений — используется для выявления уязвимостей, характерных исключительно для баз данных или веб-приложений и веб-сервисов;
- контроль политик безопасности — деятельность по контролю выполнения правил политики безопасности. Это позволяет в любой момент времени иметь актуальные сведения об элементах информационной системы, состояние которых нарушает политику безопасности, и оперативно устранять несоответствия.

Подсистема контроля эффективности защиты информации интегрируется со следующими подсистемами:

- обеспечения безопасности коммутируемой инфраструктуры и беспроводных сетей для обеспечения блокировки уязвимых узлов и узлов, не соответствующих политике информационной безопасности;
- обнаружения и предотвращения вторжений для возможности выбора способа противодействия в зависимости от критичности атаки;
- мониторинга и управления инцидентами для управления информацией об актуальных рисках, оперативного анализа и обработки наиболее критических инцидентов;
- управления обновлениями для оперативного устранения уязвимостей, связанных с отсутствием своевременно установленных обновлений безопасности.

Подсистема мониторинга и управления инцидентами ИБ

Под *событием информационной безопасности* понимается состояние системы, сервиса или сети, которое свидетельствует о возможном нарушении политики безопасности либо о прежде неизвестной ситуации, которая может иметь отношение к безопасности. *Инцидент информационной безопасности* — это одно или серия событий безопасности, которые могут привести к ущербу и потерям для организации.

Процесс управления инцидентами информационной безопасности играет важную роль в обеспечении информационной безопасности предприятия. Основной целью данного процесса является обеспечение эффективного разрешения инцидентов информационной безопасности, минимизация потерь для организации, вызванных инцидентами, и уменьшение риска возникновения повторных инцидентов.

Типовые действия, выполняемые в рамках процесса управления инцидентами информационной безопасности, включают:

- идентификацию инцидента информационной безопасности;
- реагирование на инцидент информационной безопасности;
- восстановление после инцидента информационной безопасности;

- последующие действия по инциденту (анализ первопричин возникшего инцидента, проведение служебного расследования и др.).

Автоматическое реагирование на события безопасности в соответствии с заданными правилами обработки и корреляции позволяет ускорить реакцию на возникающие инциденты ИБ и обеспечить защищенность корпоративной сети и информационных систем в круглосуточном режиме.

Средства мониторинга и управления инцидентами информационной безопасности интегрируют в себя все системы и средства защиты организации.

Подсистема обеспечения непрерывности функционирования средств защиты

Подсистема обеспечения непрерывности функционирования средств защиты включает в себя:

- резервное копирование и восстановление;
- обеспечение бесперебойного электропитания.

Система резервного копирования является служебной подсистемой системы хранения данных и предназначена для создания резервных копий и восстановления данных. Она позволяет защитить данные от разрушения не только в случае сбоев или выхода из строя аппаратуры, но и в результате ошибок программных средств и пользователей.

От надежности и стабильности системы бесперебойного питания напрямую зависит функционирование средств и систем защиты организации.

Средства обеспечения бесперебойного питания предназначены:

- для стабилизации напряжения питания, фильтрации помех и скачков напряжения;
- для обеспечения непрерывного электропитания при всех видах нарушений внешнего питания, в том числе и при полном его отключении.

Использование централизованной системы резервного копирования позволяет сократить совокупную стоимость владения системами и средствами защиты за счет оптимального использования устройств резервного копирования и сокращения расходов на администрирование (по сравнению с децентрализованной системой).

Вопросы для самоконтроля

1. Сформулируйте основополагающие принципы построения современных КИС.
2. Охарактеризуйте четыре уровня управления КИС.
3. Укажите необходимые условия обеспечения санкционированного доступа к информационным ресурсам предприятия.
4. Какие важные системные функции может выполнять КИС при реализации в ней принципа централизованного управления?

5. Объясните значение управления рисками предприятия для создания системы эффективной защиты информации на этом предприятии.
6. Какие требования необходимо учитывать при разработке архитектуры комплексной системы защиты информации?
7. Перечислите меры и средства защиты, применяемые при построении комплексной системы защиты информации КИС.
8. Укажите основные подсистемы информационной безопасности, входящие в состав КСЗИ.
9. Опишите особенности подсистемы защиты информации от несанкционированного доступа.
10. Опишите назначение и особенности подсистемы контроля эффективности защиты информации.
11. Опишите назначение и особенности подсистемы мониторинга и управления инцидентами ИБ.
12. Опишите назначение и особенности подсистемы обеспечения непрерывности функционирования средств защиты.

Глава 8
БЕЗОПАСНОСТЬ ОПЕРАЦИОННЫХ СИСТЕМ

Проблема защиты от несанкционированных действий при взаимодействии с внешними сетями может быть успешно решена только на основе комплексной защиты корпоративных информационных систем. Защищенные операционные системы относятся к базовым средствам многоуровневой комплексной защиты КИС.

8.1. Проблемы обеспечения безопасности ОС

Большинство программных средств защиты информации являются прикладными программами. Для их выполнения требуется поддержка операционной системы (ОС). Окружение, в котором функционирует ОС, называется *доверенной вычислительной базой* (ДВБ). ДВБ включает в себя полный набор элементов, обеспечивающих информационную безопасность: операционную систему, программы, сетевое оборудование, средства физической защиты и даже организационные процедуры. Краеугольным камнем этой пирамиды является защищенная операционная система. Без нее доверенная вычислительная база оказывается построенной на песке.

8.1.1. Угрозы безопасности операционной системы

Организация эффективной и надежной защиты операционной системы невозможна без предварительного анализа возможных угроз ее безопасности. Угрозы безопасности операционной системы существенно зависят от условий эксплуатации системы, от того, какая информация хранится и обрабатывается в системе, и т. д. Например, если операционная система используется для организации электронного документооборота, наиболее опасны угрозы, связанные с несанкционированным доступом (НСД) к файлам. Если же операционная система используется как платформа провайдера интернет-услуг, очень опасны атаки на сетевое программное обеспечение операционной системы.

Угрозы безопасности операционной системы можно классифицировать по различным аспектам их реализации [51, 73].

Классификация угроз *по цели атаки*:

- несанкционированное чтение информации;
- несанкционированное изменение информации;

- несанкционированное уничтожение информации;
- полное или частичное разрушение операционной системы.

Классификация угроз *по принципу воздействия на операционную систему*:

- использование известных (легальных) каналов получения информации, например угроза несанкционированного чтения файла, доступ пользователей к которому определен некорректно — разрешен доступ пользователю, которому согласно политике безопасности доступ должен быть запрещен;
- использование скрытых каналов получения информации, например угроза использования злоумышленником недокументированных возможностей операционной системы;
- создание новых каналов получения информации с помощью программных закладок.

Классификация угроз *по типу используемой злоумышленником уязвимости защиты*:

- неадекватная политика безопасности, в том числе и ошибки администратора системы;
- ошибки и недокументированные возможности программного обеспечения операционной системы, в том числе и так называемые *люки* — случайно или преднамеренно встроенные в систему «служебные входы», позволяющие обходить систему защиты;
- ранее внедренная программная закладка.

Классификация угроз по характеру *воздействия на операционную систему*:

- активное воздействие — несанкционированные действия злоумышленника в системе;
- пассивное воздействие — несанкционированное наблюдение злоумышленника за процессами, происходящими в системе.

Угрозы безопасности ОС можно также классифицировать по таким признакам, как способ действий злоумышленника, используемые средства атаки, объект атаки, способ воздействия на объект атаки, состояние атакуемого объекта ОС на момент атаки.

Операционная система может подвергнуться следующим типичным атакам:

- *сканирование файловой системы.* Злоумышленник просматривает файловую систему компьютера и пытается прочесть (или скопировать) все файлы подряд. Рано или поздно обнаруживается хотя бы одна ошибка администратора. В результате злоумышленник получает доступ к информации, который должен быть ему запрещен;
- *подбор пароля.* Существует несколько методов подбора паролей пользователей:
  - — тотальный перебор;
  - — тотальный перебор, оптимизированный по статистике встречаемости символов или с помощью словарей;

— подбор пароля с использованием знаний о пользователе (его имени, фамилии, даты рождения, номера телефона и т. д.);

- *кража ключевой информации.* Злоумышленник может подсмотреть пароль, набираемый пользователем, или восстановить набираемый пользователем пароль по движениям его рук на клавиатуре. Носитель с ключевой информацией (смарт-карта, Touch Memory и т. д.) может быть просто украден;
- *сборка мусора.* Во многих операционных системах информация, уничтоженная пользователем, не уничтожается физически, а помечается как уничтоженная (так называемый *мусор*). Злоумышленник восстанавливает эту информацию, просматривает ее и копирует интересующие его фрагменты;
- *превышение полномочий.* Злоумышленник, используя ошибки в программном обеспечении ОС или политике безопасности, получает полномочия, превышающие те, которые ему предоставлены в соответствии с политикой безопасности. Обычно это достигается путем запуска программы от имени другого пользователя;
- *программные закладки.* Программные закладки, внедряемые в операционные системы, не имеют существенных отличий от других классов программных закладок;
- *жадные программы* — это программы, преднамеренно захватывающие значительную часть ресурсов компьютера, в результате чего другие программы не могут выполняться или выполняются крайне медленно. Запуск жадной программы может привести к краху операционной системы [51, 73].

8.1.2. Понятие защищенной операционной системы

Операционную систему называют *защищенной*, если она предусматривает средства защиты от основных классов угроз. Защищенная операционная система обязательно должна содержать средства разграничения доступа пользователей к своим ресурсам, а также средства проверки подлинности пользователя, начинающего работу с операционной системой. Кроме того, защищенная операционная система должна содержать средства противодействия случайному или преднамеренному выводу операционной системы из строя.

Если операционная система предусматривает защиту не от всех основных классов угроз, а только от некоторых, такую ОС называют *частично защищенной* [51, 92].

Подходы к построению защищенных операционных систем

Существует два основных подхода к созданию защищенных операционных систем — фрагментарный и комплексный. При *фрагментарном подходе* вначале организуется защита от одной угрозы, затем от другой и т. д. Примером фрагментарного подхода может служить ситуация,

когда за основу берется незащищенная операционная система (например, Windows 98), на нее устанавливают антивирусный пакет, систему шифрования, систему регистрации действий пользователей и т. д.

При применении фрагментарного подхода подсистема защиты операционной системы представляет собой набор разрозненных программных продуктов, как правило, от разных производителей. Эти программные средства работают независимо друг от друга, при этом практически невозможно организовать их тесное взаимодействие. Кроме того, отдельные элементы такой подсистемы защиты могут некорректно работать в присутствии друг друга, что приводит к резкому снижению надежности системы.

При *комплексном подходе* защитные функции вносятся в операционную систему на этапе проектирования архитектуры операционной системы и являются ее неотъемлемой частью. Отдельные элементы подсистемы защиты, созданной на основе комплексного подхода, тесно взаимодействуют друг с другом при решении различных задач, связанных с организацией защиты информации, поэтому конфликты между ее отдельными компонентами практически невозможны. Подсистема защиты, созданная на основе комплексного подхода, может быть устроена так, что при фатальных сбоях в функционировании ее ключевых элементов она вызывает крах операционной системы, что не позволяет злоумышленнику отключать защитные функции системы. При фрагментарном подходе такая организация подсистемы защиты невозможна.

Как правило, подсистему защиты операционной системы, созданную на основе комплексного подхода, проектируют так, чтобы отдельные ее элементы были заменяемы. Соответствующие программные модули могут быть заменены другими модулями.

Административные меры защиты

Программно-аппаратные средства защиты операционной системы обязательно должны дополняться административными мерами защиты. Без постоянной квалифицированной поддержки со стороны администратора даже надежная программно-аппаратная защита может давать сбои. Перечислим основные административные меры защиты.

1. *Постоянный контроль корректности функционирования операционной системы*, особенно ее подсистемы защиты. Такой контроль удобно организовать, если операционная система поддерживает автоматическую регистрацию наиболее важных событий (event logging) в специальном журнале.

2. *Организация и поддержание адекватной политики безопасности.* Политика безопасности ОС должна постоянно корректироваться, оперативно реагируя на попытки злоумышленников преодолеть защиту операционной системы, а также на изменения в конфигурации операционной системы, установку и удаление прикладных программ.

3. *Осведомление пользователей операционной системы* о необходимости соблюдения мер безопасности при работе с ОС и контроль за соблюдением этих мер.

4. *Регулярное создание и обновление резервных копий* программ и данных ОС.

5. *Постоянный контроль изменений в конфигурационных данных и политике безопасности ОС.* Информацию об этих изменениях целесообразно хранить на неэлектронных носителях информации, для того чтобы злоумышленнику, преодолевшему защиту операционной системы, было труднее замаскировать свои несанкционированные действия.

В конкретных ОС могут потребоваться и другие административные меры защиты информации [51, 73].

Адекватная политика безопасности

Выбор и поддержание адекватной политики безопасности являются одной из наиболее важных задач администратора операционной системы. Если принятая в ОС политика безопасности неадекватна, это может привести к несанкционированному доступу злоумышленника к ресурсам системы и к снижению надежности функционирования ОС.

Известно утверждение: чем лучше защищена ОС, тем труднее с ней работать пользователям и администраторам. Это обусловлено следующими факторами:

- система защиты не всегда способна определить, является ли некоторое действие пользователя злонамеренным. Поэтому система защиты либо не пресекает некоторые виды несанкционированного доступа, либо запрещает некоторые вполне легальные действия пользователей. Чем выше защищенность системы, тем шире класс тех легальных действий пользователей, которые рассматриваются подсистемой защиты как несанкционированные;
- любая система, в которой предусмотрены функции защиты информации, требует от администраторов определенных усилий, направленных на поддержание адекватной политики безопасности. Чем больше в операционной системе защитных функций, тем больше времени и средств нужно тратить на поддержание защиты;
- подсистема защиты операционной системы, как и любой другой программный пакет, потребляет аппаратные ресурсы компьютера. Чем сложнее устроены защитные функции операционной системы, тем больше ресурсов компьютера (процессорного времени, оперативной памяти и др.) затрачивается на поддержание функционирования подсистемы защиты и тем меньше ресурсов остается на долю прикладных программ;
- поддержание слишком жесткой политики безопасности может негативно сказаться на надежности функционирования операционной системы. Чрезмерно жесткая политика безопасности может

привести к трудно выявляемым ошибкам и сбоям в процессе функционирования операционной системы и даже к краху ОС [51, 92].

Оптимальная адекватная политика безопасности — это такая политика безопасности, которая не только не позволяет злоумышленникам выполнять несанкционированные действия, но и не приводит к описанным выше негативным эффектам.

Адекватная политика безопасности определяется не только архитектурой ОС, но и ее конфигурацией, установленными прикладными программами и т. д. Формирование и поддержание адекватной политики безопасности ОС можно разделить на ряд этапов.

1. *Анализ угроз.* Администратор операционной системы рассматривает возможные угрозы безопасности данного экземпляра ОС. Среди возможных угроз выделяются наиболее опасные, защите от которых нужно уделять максимум средств.

2. *Формирование требований к политике безопасности.* Администратор определяет, какие средства и методы будут применяться для защиты от тех или иных угроз. Например, защиту от несанкционированного доступа к некоторому объекту ОС можно решать либо средствами разграничения доступа, либо криптографическими средствами, либо используя некоторую комбинацию этих средств.

3. *Формальное определение политики безопасности.* Администратор определяет, как конкретно должны выполняться требования, сформулированные на предыдущем этапе. Формулируются необходимые требования к конфигурации ОС, а также требования к конфигурации дополнительных пакетов защиты, если установка таких пакетов необходима. Результатом данного этапа является развернутый перечень настроек конфигурации ОС и дополнительных пакетов защиты с указанием того, в каких ситуациях какие настройки должны быть установлены.

4. *Претворение в жизнь политики безопасности.* Задачей данного этапа является приведение конфигурации ОС и дополнительных пакетов защиты в соответствие с политикой безопасности, формально определенной на предыдущем этапе.

5. *Поддержание и коррекция политики безопасности.* В задачу администратора на данном этапе входит контроль соблюдения политики безопасности и внесение в нее необходимых изменений по мере появления изменений в функционировании ОС.

Специальных стандартов защищенности операционных систем не существует. Для оценки защищенности операционных систем используются стандарты, разработанные для компьютерных систем вообще. Как правило, сертификация операционной системы по некоторому классу защиты сопровождается составлением требований к адекватной политике безопасности, при безусловном выполнении которой защищенность конкретного экземпляра операционной системы будет соответствовать требованиям соответствующего класса защиты.

Определяя адекватную политику безопасности, администратор операционной системы должен в первую очередь ориентироваться на защиту ОС от конкретных угроз ее безопасности [51, 92].

8.2. Архитектура подсистемы защиты операционной системы

8.2.1. Основные функции подсистемы защиты операционной системы

Подсистема защиты ОС выполняет следующие основные функции:

1. *Идентификация и аутентификация.* Ни один пользователь не может начать работу с операционной системой, не идентифицировав себя и не предоставив системе аутентифицирующую информацию, подтверждающую, что пользователь действительно является тем, кем он себя заявляет.

2. *Разграничение доступа.* Каждый пользователь системы имеет доступ только к тем объектам ОС, к которым ему предоставлен доступ в соответствии с текущей политикой безопасности.

3. *Аудит.* Операционная система регистрирует в специальном журнале события, потенциально опасные для поддержания безопасности системы.

4. *Управление политикой безопасности.* Политика безопасности должна постоянно поддерживаться в адекватном состоянии, т. е. должна гибко реагировать на изменения условий функционирования ОС. Управление политикой безопасности осуществляется администраторами системы с использованием соответствующих средств, встроенных в операционную систему.

5. *Криптографические функции.* Защита информации немыслима без использования криптографических средств защиты. Шифрование используется в ОС при хранении и передаче по каналам связи паролей пользователей и некоторых других данных, критичных для безопасности системы.

6. *Сетевые функции.* Современные ОС, как правило, работают не изолированно, а в составе локальных и/или глобальных компьютерных сетей. ОС компьютеров, входящих в одну сеть, взаимодействуют между собой для решения различных задач, в том числе имеющих прямое отношение к защите информации.

Подсистема защиты обычно не представляет собой единый программный модуль. Как правило, каждая из перечисленных функций подсистемы защиты решается одним или несколькими программными модулями. Некоторые функции встраиваются непосредственно в ядро ОС. Между различными модулями подсистемы защиты должен существовать четко определенный интерфейс, используемый при взаимодействии модулей для решения общих задач.

В таких операционных системах, как Windows XP, подсистема защиты четко выделяется в общей архитектуре ОС; в других, например UNIX, защитные функции распределены практически по всем элементам операционной системы. Однако любая ОС, удовлетворяющая стандарту защищенности, должна содержать подсистему защиты, вы-

полняющую все вышеперечисленные функции. Обычно подсистема защиты ОС допускает расширение дополнительными программными модулями [51, 92].

8.2.2. Идентификация, аутентификация и авторизация субъектов доступа

В защищенной ОС любой пользователь (субъект доступа), перед тем как начать работу с системой, должен пройти идентификацию, аутентификацию и авторизацию. Субъектом доступа (или просто субъектом) называют любую сущность, способную инициировать выполнение операций над элементами ОС. В частности, пользователи являются субъектами доступа.

Идентификация субъекта доступа заключается в том, что субъект сообщает операционной системе *идентифицирующую информацию* о себе (имя, учетный номер и т. д.) и таким образом идентифицирует себя.

Для того чтобы установить, что пользователь именно тот, за кого себя выдает, в информационных системах предусмотрена процедура аутентификации, задача которой — предотвращение доступа к системе нежелательных лиц.

Аутентификация субъекта доступа заключается в том, что субъект предоставляет операционной системе помимо идентифицирующей информации еще и *аутентифицирующую информацию*, подтверждающую, что он действительно является тем субъектом доступа, к которому относится идентифицирующая информация (см. главу 6).

Авторизация субъекта доступа происходит после успешной идентификации и аутентификации. При авторизации субъекта ОС выполняет действия, необходимые для того, чтобы субъект мог начать работу в системе. Например, авторизация пользователя в операционной системе UNIX включает в себя порождение процесса, являющегося операционной оболочкой, с которой в дальнейшем будет работать пользователь. В операционной системе Windows NT авторизация пользователя включает в себя создание маркера доступа пользователя, создание рабочего стола и запуск на нем от имени авторизуемого пользователя процесса Userinit, инициализирующего индивидуальную программную среду пользователя. Авторизация субъекта не относится напрямую к подсистеме защиты операционной системы. В процессе авторизации решаются технические задачи, связанные с организацией начала работы в системе уже идентифицированного и аутентифицированного субъекта доступа.

С точки зрения обеспечения безопасности ОС процедуры идентификации и аутентификации являются весьма ответственными. Действительно, если злоумышленник сумел войти в систему от имени другого пользователя, он легко получает доступ ко всем объектам ОС, к которым имеет доступ этот пользователь. Если при этом подсистема аудита генерирует сообщения о событиях, потенциально опасных для

безопасности ОС, то в журнал аудита записывается не имя злоумышленника, а имя пользователя, от имени которого злоумышленник работает в системе.

Наиболее распространенными методами идентификации и аутентификации являются следующие:

- идентификация и аутентификация с помощью имени и пароля;
- идентификация и аутентификация с помощью внешних носителей ключевой информации;
- идентификация и аутентификация с помощью биометрических характеристик пользователей.

Перечисленные выше методы идентификации и аутентификации подробно рассмотрены в главе 5.

8.2.3. Разграничение доступа к объектам операционной системы

Основными понятиями процесса разграничения доступа к объектам операционной системы являются объект доступа, метод доступа к объекту и субъект доступа [51, 92].

Объектом доступа (или просто *объектом*) называют любой элемент операционной системы, доступ к которому пользователей и других субъектов доступа может быть произвольно ограничен. Возможность доступа к объектам ОС определяется не только архитектурой операционной системы, но и текущей политикой безопасности. Под объектами доступа понимают как ресурсы оборудования (процессор, сегменты памяти, принтер, диски и ленты), так и программные ресурсы (файлы, программы, семафоры), т. е. все то, доступ к чему контролируется. Каждый объект имеет уникальное имя, отличающее его от других объектов в системе, и может быть доступен через хорошо определенные и значимые операции.

Методом доступа к объекту называется операция, определенная для объекта. Тип операции зависит от объектов. Например, процессор может только выполнять команды, сегменты памяти могут быть записаны и прочитаны, считыватель магнитных карт может только читать, а для файлов могут быть определены методы доступа «чтение», «запись» и «добавление» (дописывание информации в конец файла).

Субъектом доступа называют любую сущность, способную инициировать выполнение операций над объектами (обращаться к объектам по некоторым методам доступа). Обычно полагают, что множество субъектов доступа и множество объектов доступа не пересекаются.

Иногда к субъектам доступа относят процессы, выполняющиеся в системе. Однако логичнее считать субъектом доступа именно пользователя, от имени которого выполняется процесс. Естественно, под субъектом доступа подразумевают не физического пользователя, работающего с компьютером, а «логического», от имени которого выполняются процессы операционной системы.

Таким образом, *объект доступа* — это то, к чему осуществляется доступ, *субъект доступа* — это тот, кто осуществляет доступ, и *метод доступа* — это то, как осуществляется доступ.

Для объекта доступа может быть определен *владелец* — субъект, которому принадлежит данный объект и который несет ответственность за конфиденциальность содержащейся в объекте информации, а также за целостность и доступность объекта.

Обычно владельцем объекта автоматически назначается субъект, создавший данный объект; в дальнейшем владелец объекта может быть изменен с использованием соответствующего метода доступа к объекту. На владельца, как правило, возлагается ответственность за корректное ограничение прав доступа к данному объекту других субъектов.

Правом доступа к объекту называют право на получение доступа к объекту по некоторому методу или группе методов. Например, если пользователь имеет возможность читать файл, говорят, что он имеет право на чтение этого файла. Говорят, что субъект имеет некоторую *привилегию,* если он имеет право на доступ по некоторому методу или группе методов ко всем объектам ОС, поддерживающим данный метод доступа.

Разграничением доступа субъектов к объектам является совокупность правил, определяющая для каждой тройки субъект—объект—метод, разрешен ли доступ данного субъекта к данному объекту по данному методу. При избирательном разграничении доступа возможность доступа определена однозначно для каждой тройки субъект—объект—метод, при полномочном разграничении доступа ситуация несколько сложнее.

Субъекта доступа называют *суперпользователем,* если он имеет возможность игнорировать правила разграничения доступа к объектам.

Правила разграничения доступа

Правила разграничения доступа, действующие в операционной системе, устанавливаются администраторами системы при определении текущей политики безопасности. За соблюдением этих правил субъектами доступа следит *монитор ссылок* — часть подсистемы защиты операционной системы.

Правила разграничения доступа должны удовлетворять следующим требованиям:

1. Правила разграничения доступа, принятые в операционной системе, должны соответствовать аналогичным правилам, принятым в организации, в которой установлена эта ОС. Иными словами, если согласно правилам организации доступ пользователя к некоторой информации считается несанкционированным, этот доступ должен быть ему запрещен.

2. Правила разграничения доступа не должны допускать разрушающие воздействия субъектов доступа на ОС, выражающиеся в несанкционированном изменении, удалении или другом воздействии на объекты, жизненно важные для нормальной работы ОС.

3. Любой объект доступа должен иметь владельца. Недопустимо присутствие *ничейных объектов* — объектов, не имеющих владельца.

4. Недопустимо присутствие *недоступных объектов* — объектов, к которым не может обратиться ни один субъект доступа ни по одному методу доступа.

5. Недопустима утечка конфиденциальной информации.

Основные модели разграничения доступа

Существуют две основные модели разграничения доступа:

- избирательное (дискреционное) разграничение доступа;
- полномочное (мандатное) разграничение доступа.

При *избирательном разграничении доступа* (Discretionary Access Control) определенные операции над конкретным ресурсом запрещаются или разрешаются субъектам или группам субъектов. Большинство операционных систем реализуют именно избирательное разграничение доступа.

Полномочное разграничение доступа заключается в том, что все объекты могут иметь уровни секретности, а все субъекты делятся на группы, образующие иерархию в соответствии с уровнем допуска к информации. Иногда эту модель называют моделью многоуровневой безопасности, предназначенной для хранения секретов.

Избирательное разграничение доступа

Система правил избирательного разграничения доступа формулируется следующим образом.

1. Для любого объекта операционной системы существует владелец.

2. Владелец объекта может произвольно ограничивать доступ других субъектов к данному объекту.

3. Для каждой тройки субъект—объект—метод возможность доступа определена однозначно.

4. Существует хотя бы один привилегированный пользователь (администратор), имеющий возможность обратиться к любому объекту по любому методу доступа.

Этот привилегированный пользователь не может игнорировать разграничение доступа к объектам. Например, в Windows NT администратор для обращения к чужому объекту (принадлежащему другому субъекту) должен вначале объявить себя владельцем этого объекта, использовав привилегию администратора объявлять себя владельцем любого объекта, затем дать себе необходимые права, и только после этого администратор может обратиться к объекту. Последнее требование введено для реализации механизма удаления потенциально недоступных объектов.

При создании объекта его владельцем назначается субъект, создавший данный объект. В дальнейшем субъект, обладающий необходимы-

ми правами, может назначить объекту нового владельца. При этом субъект, изменяющий владельца объекта, может назначить новым владельцем объекта только себя. Такое ограничение вводится для того, чтобы владелец объекта не мог отдать владение объектом другому субъекту и тем самым снять с себя ответственность за некорректные действия с объектом.

Для определения прав доступа субъектов к объектам при избирательном разграничении доступа используются такие понятия, как *матрица доступа* и домен безопасности.

С концептуальной точки зрения текущее состояние прав доступа при избирательном разграничении доступа описывается матрицей, в строках которой перечислены субъекты доступа, в столбцах — объекты доступа, а в ячейках — операции, которые субъект может выполнить над объектом.

Домен безопасности (Protection Domain) определяет набор объектов и типов операций, которые могут производиться над каждым объектом операционной системы.

Возможность выполнять операции над объектом есть *право доступа*, представляющее собой упорядоченную пару <object-name, rights-set>. Таким образом, *домен есть набор прав доступа*. Например, если домен D имеет право доступа <file F, {read, write}>, это означает, что процесс, выполняемый в домене D, может читать или писать в файл F, но не может выполнять других операций над этим объектом. Пример доменов показан в табл. 8.1.

Таблица 8.1. **Специфицирование прав доступа к ресурсам**

Домен	Объект			
	F1	F2	F3	Printer
D1	read		execute	
D2		read		
D3				print
D4	read write		read write	

Связь конкретных субъектов, функционирующих в операционных системах, может быть организована следующим образом:

- каждый пользователь может быть доменом. В этом случае набор объектов, к которым может быть организован доступ, зависит от *идентификации пользователя*;
- каждый процесс может быть доменом. В этом случае набор доступных объектов определяется *идентификацией процесса*;
- каждая процедура может быть доменом. В этом случае набор доступных объектов соответствует локальным переменным, определенным внутри процедуры. Заметим, что когда процедура выполнена, происходит смена домена.

Рассмотрим стандартную двухрежимную модель выполнения ОС. Когда процесс выполняется в *режиме системы* (Kernel Mode), он может вызывать привилегированные инструкции и иметь полный контроль над компьютерной системой. С другой стороны, если процесс выполняется в *пользовательском режиме* (User Domain), он может вызывать только непривилегированные инструкции. Следовательно, он может выполняться только внутри предопределенного пространства памяти. Наличие этих двух режимов позволяет защитить ОС (Kernel Domain) от пользовательских процессов (выполняющихся в режиме User Domain). В мультипрограммных системах двух доменов недостаточно, так как появляется необходимость защиты пользователей друг от друга.

В ОС UNIX домен связан с пользователем. Каждый пользователь обычно работает со своим набором объектов.

Модель безопасности, специфицированная выше (см. табл. 8.1), имеет вид матрицы и называется *матрицей доступа*. Столбцы этой матрицы представляют собой объекты, строки — субъекты. В каждой ячейке матрицы хранится совокупность прав доступа, предоставленных данному субъекту на данный объект. Поскольку реальная матрица доступа очень велика (типичный объем для современной операционной системы составляет несколько десятков мегабайтов), ее никогда не хранят в системе в явном виде. В общем случае эта матрица будет разреженной, т. е. большинство ее клеток будут пустыми. Матрицу доступа можно разложить по столбцам, в результате чего получаются *списки прав доступа* ACL (Access Control List). В результате разложения матрицы по строкам получаются *мандаты возможностей* (Capability List или Capability Tickets).

Список прав доступа ACL. Каждая колонка в матрице может быть реализована как список доступа для одного объекта. Очевидно, что пустые клетки могут не учитываться. В результате для каждого объекта имеем список упорядоченных пар <domain, rights-set>, который определяет все домены с непустыми наборами прав для данного объекта.

Элементами списка прав доступа ACL могут быть процессы, пользователи или группы пользователей. При реализации широко применяется предоставление доступа по умолчанию для пользователей, права которых не указаны. Например, в ОС UNIX все субъекты-пользователи разделены на три группы (владелец, группа и остальные) и для членов каждой группы контролируются операции чтения, записи и исполнения (rwx). В итоге имеем ACL — 9-битный код, который является атрибутом разнообразных объектов UNIX.

Мандаты возможностей. Как отмечалось выше, если матрицу доступа хранить по строкам, т. е. если каждый субъект хранит список объектов и для каждого объекта — список допустимых операций, то такой способ хранения называется мандатами возможностей, или перечнями возможностей. Каждый пользователь обладает несколькими мандатами и может иметь право передавать их другим. Мандаты могут быть рассеяны по системе и вследствие этого представлять бо́льшую угрозу для безопасности, чем списки контроля доступа. Их хранение должно быть

тщательно продумано. Примерами систем, использующих перечни возможностей, являются Hydra, Cambridge CAP System.

Избирательное разграничение доступа является наиболее распространенным способом разграничения доступа. Это обусловлено его сравнительной простотой реализации и необременительностью правил такого разграничения доступа для пользователей. Главное достоинство избирательного разграничения доступа — гибкость; основные недостатки — рассредоточенность управления и сложность централизованного контроля.

Вместе с тем защищенность операционной системы, подсистема защиты которой реализует только избирательное разграничение доступа, в некоторых случаях может оказаться недостаточной. В частности, в США запрещено хранить информацию, содержащую государственную тайну, в компьютерных системах, поддерживающих только избирательное разграничение доступа.

Расширением модели избирательного разграничения доступа является *изолированная (или замкнутая) программная среда.*

Изолированная программная среда. При использовании изолированной программной среды права субъекта на доступ к объекту определяются не только правами и привилегиями субъекта, но и процессом, с помощью которого субъект обращается к объекту. Можно, например, разрешить обращаться к файлам с расширением .doc только программам Word, Word Viewer и WPview.

Система правил разграничения доступа для модели изолированной программной среды формулируется следующим образом:

1. Для любого объекта операционной системы существует владелец.
2. Владелец объекта может произвольно ограничивать доступ других субъектов к данному объекту.
3. Для каждой четверки субъект—объект—метод—процесс возможность доступа определена однозначно.
4. Существует хотя бы один привилегированный пользователь (администратор), имеющий возможность обратиться к любому объекту по любому методу.
5. Для каждого субъекта определен список программ, которые этот субъект может запускать [51].

Изолированная программная среда существенно повышает защищенность операционной системы от разрушающих программных воздействий, включая программные закладки и компьютерные вирусы. Кроме того, при использовании данной модели повышается защищенность целостности данных, хранящихся в системе. В то же время изолированная программная среда создает определенные сложности в администрировании операционной системы. Например, при установке нового программного продукта администратор должен изменить списки разрешенных программ для пользователей, которые должны иметь возможность работать с этим программным продуктом. Изолированная программная среда не защищает от утечки конфиденциальной информации.

Полномочное разграничение доступа с контролем информационных потоков

Полномочное, или мандатное, разграничение доступа (Mandatory Access Control) обычно применяется в совокупности с избирательным разграничением доступа. Рассмотрим именно такой случай [51]. Правила разграничения доступа в данной модели формулируются следующим образом:

1. Для любого объекта операционной системы существует владелец.
2. Владелец объекта может произвольно ограничивать доступ других субъектов к данному объекту.
3. Для каждой четверки субъект—объект—метод—процесс возможность доступа определена однозначно в каждый момент времени. При изменении состояния процесса со временем возможность предоставления доступа также может измениться. Вместе с тем в каждый момент времени возможность доступа определена однозначно. Поскольку права процесса на доступ к объекту меняются с течением времени, они должны проверяться не только при открытии объекта, но и перед выполнением над объектом таких операций, как чтение и запись.
4. Существует хотя бы один привилегированный пользователь (администратор), имеющий возможность удалить любой объект.
5. В множестве объектов выделяется множество *объектов полномочного разграничения доступа.* Каждый объект полномочного разграничения доступа имеет гриф секретности. Чем выше числовое значение грифа секретности, тем секретнее объект. Нулевое значение грифа секретности означает, что объект несекретен. Если объект не является объектом полномочного разграничения доступа или несекретен, администратор может обратиться к нему по любому методу, как и в предыдущей модели разграничения доступа.
6. Каждый субъект доступа имеет *уровень допуска.* Чем выше числовое значение уровня допуска, тем больший допуск имеет субъект. Нулевое значение уровня допуска означает, что субъект не имеет допуска. Обычно ненулевое значение допуска назначается только субъектам-пользователям и не назначается субъектам, от имени которых выполняются системные процессы.
7. Доступ субъекта к объекту должен быть запрещен независимо от состояния матрицы доступа, если:
   - объект является объектом полномочного разграничения доступа;
   - гриф секретности объекта строго выше уровня допуска субъекта, обращающегося к нему;
   - субъект открывает объект в режиме, допускающем чтение информации.

Это правило называют *правилом NRU (Not Read Up — не читать выше).*

8. Каждый процесс операционной системы имеет *уровень конфиденциальности,* равный максимуму из грифов секретности объектов, открытых процессом на протяжении своего существования. Уровень кон-

фиденциальности фактически представляет собой гриф секретности информации, хранящейся в оперативной памяти процесса.

9. Доступ субъекта к объекту должен быть запрещен независимо от состояния матрицы доступа, если:

- объект является объектом полномочного разграничения доступа;
- гриф секретности объекта строго ниже уровня конфиденциальности процесса, обращающегося к нему;
- субъект собирается записывать в объект информацию.

Это правило разграничения доступа предотвращает утечку секретной информации. Это — так называемое *правило NWD (Not Write Down — не записывать ниже).*

10. Понизить гриф секретности объекта полномочного разграничения доступа может только субъект, который:

- имеет доступ к объекту согласно правилу 7;
- обладает специальной привилегией, позволяющей ему понижать грифы секретности объектов.

При использовании данной модели разграничения доступа существенно страдает производительность операционной системы, поскольку права доступа к объекту должны проверяться не только при открытии объекта, но и при каждой операции чтения/записи.

Кроме того, данная модель разграничения доступа создает пользователям определенные неудобства, связанные с тем, что если уровень конфиденциальности процесса строго выше нуля, то вся информация в памяти процесса фактически является секретной и не может быть записана в несекретный объект.

Если процесс одновременно работает с двумя объектами, только один из которых является секретным, процесс не может записывать информацию из памяти во второй объект. Эта проблема решается посредством использования специального программного интерфейса API для работы с памятью. Области памяти, выделяемые процессам, могут быть описаны как объекты полномочного разграничения доступа, после чего им могут назначаться грифы секретности.

При чтении секретного файла процесс должен считать содержимое такого файла в секретную область памяти, используя для этого функции операционной системы, гарантирующие невозможность утечки информации. Для работы с секретной областью памяти процесс также должен использовать специальные функции. Поскольку утечка информации из секретных областей памяти в память процесса невозможна, считывание процессом секретной информации в секретные области памяти не отражается на уровне конфиденциальности процесса. Если же процесс считывает секретную информацию в область памяти, не описанную как объект полномочного разграничения доступа, повышается уровень конфиденциальности процесса.

Из вышеизложенного следует, что пользователи операционных систем, реализующих данную модель разграничения доступа, вынуждены использовать программное обеспечение, разработанное с учетом этой модели. В противном случае пользователи будут испытывать серьезные

проблемы в процессе работы с объектами операционной системы, имеющими ненулевой гриф секретности.

Определенные проблемы вызывает также вопрос о назначении грифов секретности создаваемым объектам. Если пользователь создает новый объект с помощью процесса, имеющего ненулевой уровень конфиденциальности, пользователь вынужден присвоить новому объекту гриф секретности не ниже уровня конфиденциальности процесса. Во многих ситуациях это неудобно.

Модель полномочного разграничения доступа без контроля информационных потоков уступает по всем параметрам модели избирательного разграничения доступа, поэтому ее рассмотрение не проводилось [51].

Сравнительный анализ моделей разграничения доступа

Каждая из рассмотренных моделей разграничения доступа имеет свои достоинства и недостатки. Таблица 8.2 позволяет провести их сравнительный анализ.

Таблица 8.2. **Модели разграничения доступа**

Свойства модели	Избирательное разграничение доступа	Изолированная программная среда	Полномочное разграничение доступа с контролем потоков
Защита от утечки информации	Отсутствует	Отсутствует	Имеется
Защищенность от разрушающих воздействий	Низкая	Высокая	Низкая
Сложность реализации	Низкая	Средняя	Высокая
Сложность администрирования	Низкая	Средняя	Высокая
Затраты ресурсов компьютера	Низкие	Низкие	Высокие
Использование ПО, разработанного для других систем	Возможно	Возможно	Проблематично

Как видно из табл. 8.2, в большинстве ситуаций применение избирательного разграничения доступа наиболее эффективно. Изолированную программную среду целесообразно использовать в случаях, когда важно обеспечить целостность программ и данных операционной системы. Полномочное разграничение доступа с контролем информационных потоков следует применять в тех случаях, когда для организации чрезвычайно важно обеспечение защищенности системы от несанкционированной утечки информации. В остальных ситуациях применение этой модели нецелесообразно из-за резкого ухудшения эксплуатационных качеств операционной системы.

8.2.4. Аудит

Процедура *аудита* применительно к ОС заключается в регистрации в специальном журнале, называемом *журналом аудита*, или *журналом безопасности*, событий, которые могут представлять опасность для опе-

рационной системы. Пользователи системы, обладающие правом чтения журнала аудита, называются *аудиторами* [51, 92].

Необходимость включения в защищенную операционную систему функций аудита обусловлена следующими обстоятельствами:

- обнаружение попыток вторжения является важнейшей задачей системы защиты, поскольку ее решение позволяет минимизировать ущерб от взлома и собирать информацию о методах вторжения;
- подсистема защиты ОС может не отличить случайные ошибки пользователей от злонамеренных действий. Администратор, просматривая журнал аудита, сможет установить, что произошло при вводе пользователем неправильного пароля — ошибка легального пользователя или атака злоумышленника. Если пользователь пытался угадать пароль 20—30 раз — это явная попытка подбора пароля;
- администраторы ОС должны иметь возможность получать информацию не только о текущем состоянии системы, но и о том, как ОС функционировала в недавнем прошлом. Такую возможность обеспечивает журнал аудита;
- если администратор ОС обнаружил, что против системы проведена успешная атака, ему важно выяснить, когда была начата атака и каким образом она осуществлялась. Журнал аудита может содержать всю необходимую информацию.

К числу событий, которые могут представлять опасность для операционной системы, обычно относят следующие:

- вход или выход из системы;
- операции с файлами (открыть, закрыть, переименовать, удалить);
- обращение к удаленной системе;
- смена привилегий или иных атрибутов безопасности (режима доступа, уровня благонадежности пользователя и т. п.).

Если фиксировать в журнале аудита все события, объем регистрационной информации будет расти слишком быстро, что затруднит ее эффективный анализ. Необходимо предусмотреть выборочное протоколирование как в отношении пользователей, так и в отношении событий.

Требования к аудиту

Подсистема аудита операционной системы должна удовлетворять следующим требованиям:

1. Добавлять записи в журнал аудита может только операционная система. Если предоставить это право какому-то физическому пользователю, этот пользователь получит возможность компрометировать других пользователей, добавляя в журнал аудита соответствующие записи.

2. Редактировать или удалять отдельные записи в журнале аудита не может ни один субъект доступа, в том числе и сама ОС.

3. Просматривать журнал аудита могут только пользователи, обладающие соответствующей привилегией.

4. Очищать журнал аудита могут только пользователи-аудиторы. После очистки журнала в него автоматически вносится запись о том, что журнал аудита был очищен, с указанием времени очистки журнала и имени пользователя, очистившего журнал. Операционная система должна поддерживать возможность сохранения журнала аудита перед очисткой в другом файле.

5. При переполнении журнала аудита ОС аварийно завершает работу («зависает»). После перезагрузки работать с системой могут только аудиторы. Операционная система переходит к обычному режиму работы только после очистки журнала аудита.

Для ограничения доступа к журналу аудита должны применяться специальные средства защиты.

Политика аудита

Политика аудита — это совокупность правил, определяющих то, какие события должны регистрироваться в журнале аудита. Для обеспечения надежной защиты операционной системы в журнале аудита должны обязательно регистрироваться следующие события:

- попытки входа/выхода пользователей из системы;
- попытки изменения списка пользователей;
- попытки изменения политики безопасности, в том числе и политики аудита.

Окончательный выбор того, какие события должны регистрироваться в журнале аудита, а какие не должны, возлагается на аудиторов. При выборе оптимальной политики аудита следует учитывать ожидаемую скорость заполнения журнала аудита. Политика аудита должна оперативно реагировать на изменения в конфигурации операционной системы, в характере хранимой и обрабатываемой информации, а особенно на выявленные попытки атаки операционной системы.

В некоторых ОС подсистема аудита помимо записи информации о зарегистрированных событиях в специальный журнал предусматривает возможность интерактивного оповещения аудиторов об этих событиях.

8.3. Обеспечение безопасности ОС UNIX

8.3.1. Основные положения

Операционная система UNIX (ОС UNIX) широко используется во всех областях, в том числе в организациях, где безопасности информации уделяется особое внимание. При этом следует отметить, что при разработке UNIX более четверти века назад она не предназначалась для защиты информации. Это не означает, что современные реализации UNIX не обеспечивают полноценную реализацию механизмов безопасности. Первоначально заложенные в UNIX решения по защите инфор-

мации, такие как идентификация пользователей и разграничение доступа, с некоторыми дополнениями успешно используются и сегодня при построении защищенных систем.

Большинство систем UNIX по уровню безопасности удовлетворяют требованиям класса C2, сформулированным в *Оранжевой книге* «Критерии безопасности компьютерных систем» Министерства обороны США. Приведем требования класса C2 оранжевой книги:

- каждый пользователь должен быть идентифицирован уникальным входным именем и паролем для входа в систему. Доступ к компьютеру предоставляется лишь после аутентификации;
- система должна быть в состоянии использовать эти уникальные идентификаторы, чтобы следить за действиями пользователя (управление избирательным доступом). Владелец ресурса (например, файла) должен иметь возможность контролировать доступ к этому ресурсу;
- операционная система должна защищать объекты от повторного использования. Перед выделением новому пользователю все объекты, включая память и файлы, должны инициализироваться;
- системный администратор должен иметь возможность вести учет всех событий, относящихся к безопасности;
- система должна защищать себя от внешнего влияния или навязывания, такого как модификация загруженной системы или системных файлов, хранящихся на диске.

Сегодня на смену Оранжевой книге пришли международный стандарт ISO 15408 «Общие критерии безопасности информационных технологий» и отечественный стандарт ГОСТ Р ИСО/МЭК 15408, а критерии класса C2 сменил набор критериев Controlled Access Protection Profile.

Изначально ОС UNIX разрабатывалась как открытая система, поэтому она не могла не унаследовать некоторые элементы открытости. В силу этого при конфигурации системы UNIX возникает определенный набор ситуаций, которые могут приводить к нарушению механизмов безопасности. Поэтому для обеспечения безопасности ОС UNIX принципиально важны ее правильная конфигурация и настройка. Чтобы правильно настроить систему, администратор должен четко учитывать все требования, которые описаны в политике безопасности предприятия. Определив потенциальные угрозы, необходимо выяснить, какие средства существуют для обеспечения и развития защиты в ОС UNIX. При этом, учитывая вычислительные и материальные затраты на обеспечение безопасности, надо строить систему защиты в соответствии с принципом разумной достаточности.

Следующей причиной нарушений безопасности ОС UNIX является наличие некорректно работающих программ, которые при некоторых нештатных ситуациях выполняют ряд дополнительных незапланированных действий. Ни один производитель программного обеспечения не дает 100-процентную гарантию своего продукта, поскольку всегда остается определенное количество невыявленных ошибок. Ясно, что все это относится и к ОС UNIX. Следует отметить, что производители

систем UNIX весьма оперативно реагируют на сообщения об ошибках и зарегистрированные пользователи могут их легко исправить.

Не существует компьютерной системы, в которой риск нарушений безопасности сведен к нулю, поэтому принято употреблять термин «надежная» (trusted)) вместо «безопасная» (secure). *Надежной системой* называют систему, в которой достигается некоторый уровень контроля над доступом к информации, обеспечивающий механизмы предотвращения или по крайней мере фиксирования несанкционированного доступа.

Под предотвращением несанкционированного доступа понимают поддержку заданного уровня конфиденциальности (невозможности несанкционированного получения информации), целостности (невозможности несанкционированной ее модификации) и доступности (невозможности получения информации за разумное время).

Для защиты ОС UNIX могут применяться как базовые средства, так и расширенные средства стандартных систем. При этом расширенные средства защиты должны быть полностью совместимы с базовыми механизмами защиты ОС UNIX.

Основное решение, принимаемое на начальном этапе установки системы, — определение числа администраторов, которые будут сопровождать систему. Существует два принципиально разных решения: иметь одного суперпользователя с именем `root` с неограниченными правами или нескольких пользователей с распределенными административными обязанностями.

В надежной системе UNIX роль администратора распадается на несколько логических ролей, каждая из которых предполагает ответственность за определенный сервис системы. Идея о специфических административных ролях и соответствующих им задачах и обязанностях является основной в понятии надежной операционной системы. В ОС UNIX любая логическая роль может быть назначена одному и тому же пользователю или различным членам некоторой административной группы пользователей. Каждая расширенная роль имеет свою авторизацию. Эта связь позволяет администратору вести полную регистрацию административных действий.

Например, в операционной системе SCO UNIX Release 5.0 существуют следующие администраторы:

- администратор системных утилит (System daemons);
- администратор системных команд (Owner of system command);
- администратор системных файлов (Owner of system files);
- администратор учета пользователей и терминалов (System accounting);
- администратор службы UUCP (UUCP administrator);
- администратор службы аутентификации (Authentication administrator);
- администратор системы cron (Cron daemon);
- администратор почты (Mmdf or Sendmail administrator);
- администратор сети, организованной через порты (Micnet administrator);

- администратор печати (Printer administrator);
- администратор аудита (Audit administrator).

При введении дополнительных компонентов системы (СУБД, различных видов сервиса и т. д.) в системе появляются соответствующие администраторы.

Все администраторы вместе выполняют функции суперпользователя. При этом, если использовать предлагаемую политику безопасности, суперпользователь может логически отсутствовать в системе. Пароль суперпользователя можно ввести с помощью нескольких человек, причем никто из них не будет знать пароль, получившийся в результате. Такая схема позволяет четко разделить обязанности и ответственность между людьми, которые администрируют и поддерживают работу системы.

В дальнейшем изложении материала, где это возможно по смыслу, будет использоваться термин «администратор» без уточнения его функций.

Заметим, что средства обеспечения безопасности в ОС UNIX будут бесполезны, если не реализованы организационные меры защиты.

8.3.2. Парольная защита

Пароль — наиболее важная часть обеспечения безопасности системы UNIX. Если злоумышленник узнает пароль пользователя, он может работать с правами этого пользователя, в том числе и суперпользователя.

Рассмотрим стандартную процедуру идентификации и аутентификации пользователя в ОС UNIX. Система ищет имя пользователя в файле /etc/passwd, и если пользователь идентифицируется, то аутентификация заключается в сравнении введенного пароля с тем, который хранится в зашифрованном виде. При этом предусмотрено выполнение некоторых правил относительно характеристик пароля и возможности его изменения. Однако этих правил недостаточно для реализации надежной защиты.

В надежной системе стандартная процедура идентификации и аутентификации расширена. В ней предусмотрено больше правил, касающихся типов используемых паролей. Введены процедуры генерации и смены паролей. Изменены местоположение и механизм защиты некоторых частей базы данных паролей. Администратору аутентификации предоставлены дополнительные возможности для контроля действий пользователей.

Для безопасности систем UNIX чрезвычайно важны правила выбора безопасных паролей. Для реализации правил использования безопасных паролей в UNIX (в SCO UNIX Release 5.0, в частности) существуют следующие средства:

1. Задание администратором учета пользователей и терминалов определенных требований к паролям:

- ограничение минимальной длины вводимого пользователем пароля;

- требование наличия в пароле обязательного минимального количества букв нижнего регистра, букв верхнего регистра, цифр и специальных символов;
- запрещение пользователю введения собственных паролей; разрешение вводить только пароли, сгенерированные системой.

2. Задание администратором временных ограничений по частоте сменяемости и времени жизни паролей. При этом для удобства пользователя возможно задание интервала времени между началом требования смены пароля и окончанием срока его действия.

3. Автоматическое блокирование входа пользователя в систему при старости пароля и при определенном числе неуспешных попыток входа.

4. Задание каждому пользователю количества и номеров терминалов для входа в систему.

5. Проверка системой паролей пользователей на стойкость при их вводе (вхождение идентификатора, имени пользователя, повторяемость символов и т. д.).

6. Хранение зашифрованных паролей не в /etc/passwd, как в старых версиях, а в закрытом от доступа отдельном файле.

7. Получение статистической информации о времени работы пользователя в системе, его блокировках, номерах терминалов и т. д.

8. При установке класса защиты C2 невозможность администратором регистрировать пользователя без пароля (guest — гость).

Помимо этого существует возможность блокирования по числу неуспешных попыток входа не только пользователя, но и терминала. При этом можно задать интервал времени между попытками регистрации. Также предусмотрено ведение записей об успешных и неуспешных попытках входа в систему.

Хорошо себя зарекомендовало использование командного интерпретатора rsh (restricted). Во-первых, пользователь не может никуда перейти из своего домашнего справочника. Во-вторых, он может использовать только команды из тех справочников, которые определены в переменной окружения `PATH`. При этом изменить значение переменной окружения `PATH` пользователь не может. В-третьих, пользователь не может задавать полные имена программных файлов и перенаправлять потоки ввода-вывода.

Можно еще больше ограничить действия пользователя путем введения в его стартовый командный файл (.profile) определенной команды (системы, приложения), которая будет вызываться через команду `exec`. В этой ситуации если в стартовый командный файл добавить команды `trap` и `exit`, то пользователь сможет работать только с заданной ему командой (системой).

Следует отметить, что успешная реализация любой защиты, в том числе и парольной, возможна только при строгом соблюдении организационных мер. При этом реальной угрозой преодоления парольной защиты является нарушение такой организационной меры защиты, как оставление без присмотра терминала, на котором пользователь уже зарегистрировался. В этом случае необходимо проводить работу с пользо-

вателями, чтобы они применяли команды блокирования терминала (`lock`, `xlock`).

Существуют средства автоматического блокирования терминала по истечении определенного периода времени. Такие средства встроены в некоторые командные интерпретаторы или графические оболочки. Однако использование этих средств нецелесообразно из-за опасности внедрения программы, имитирующей блокирование экрана и считывающей пароль пользователя. Заметим также, что в системе должен быть определен список терминалов, с которых не могут входить в систему администраторы.

Парольная защита применяется также для того, чтобы обезопасить удаленный вход пользователей по каналам связи, подключаемым к последовательным портам. В этом случае возможна установка отдельного пароля на каждое используемое для удаленного входа устройство (специальный файл). При вводе неправильного пароля с удаленной системы работа с системой UNIX невозможна.

Корректная реализация администратором средств парольной защиты, предоставляемых системой UNIX , позволяет гарантировать целостность парольной защиты при соблюдении организационных мер безопасности.

8.3.3. Защита файловой системы

Наибольшее внимание в проблеме защиты операционной системы необходимо уделять защите файловой системы [89, 92]. Все пользователи ОС UNIX явно или неявно работают с файлами.

Файловая система ОС UNIX имеет древовидную структуру. Промежуточными узлами дерева являются каталоги со ссылками на другие каталоги или файлы, а листья дерева соответствуют файлам или пустым каталогам.

По отношению к конкретному файлу все пользователи делятся на три категории:

- владелец файла;
- члены группы владельца;
- прочие пользователи.

Для каждой из этих категорий режим доступа определяет права на операции с файлом, а именно:

- право на чтение;
- право на запись;
- право на выполнение (для каталогов — право на поиск).

В итоге девяти (3 × 3) битов защиты оказывается достаточно, чтобы специфицировать ACL каждого файла. Аналогичным образом защищены и другие объекты ОС UNIX, например семафоры, сегменты разделяемой памяти и т. п.

Каждый файл в системе UNIX имеет уникальный индекс. Индекс — это управляющий блок. В литературе он также называется ин-

дексным дескриптором, i-node или i-узлом. Индекс содержит информацию, необходимую любому процессу для того, чтобы обратиться к файлу, например права собственности на файл, права доступа к файлу, размер файла и расположение данных файла в файловой системе.

Процессы обращаются к файлам, используя четко определенный набор системных вызовов и идентифицируя файл строкой символов, выступающих в качестве составного имени файла. Каждое составное имя однозначно определяет файл, благодаря чему ядро системы преобразует это имя в индекс файла.

Индексы существуют на диске в статической форме, и ядро считывает их в память, прежде чем начать с ними работать. Индексы содержат следующие поля:

1. Идентификатор владельца файла и идентификатор группы.
2. Тип файла. Файл может быть файлом обычного типа, каталогом, специальным файлом (соответствующим устройствам ввода-вывода символами или блоками, а также абстрактным файлом канала, организующим обслуживание запросов в порядке поступления — «первым пришел — первым вышел»).
3. Права доступа к файлу. Права доступа к файлу разделены между индивидуальным владельцем, группой пользователей, в которую входит владелец файла, и всеми остальными. Суперпользователь (пользователь с именем `root`) имеет право доступа ко всем файлам в системе. Каждому классу пользователей выделены определенные права на чтение, запись и выполнение файла, которые устанавливаются индивидуально. Поскольку каталоги как файлы не могут быть исполнены, разрешение на исполнение в данном случае интерпретируется как право производить поиск в каталоге по имени файла, а право записи — как возможность создавать и уничтожать в нем файлы.
4. Временные сведения, характеризующие работу с файлом: время внесения последних изменений в файл, время последнего обращения к файлу, время внесения последних изменений в индекс.
5. Число указателей индекса, означающее количество имен файлов, ссылающихся на данный файл.
6. Таблицу адресов дисковых блоков, в которых располагается информация файла. Хотя пользователи трактуют информацию в файле как логический поток байтов, ядро располагает эти данные в несмежных дисковых блоках.
7. Размер файла в байтах.

Обратим внимание, что в индексе отсутствует составное имя файла, необходимое для доступа к файлу. *Составное имя* — это строка символов, завершающаяся пустым символом и разделяемая наклонной чертой (/) на несколько компонентов. Каждый компонент, кроме последнего, должен быть именем каталога, но последний компонент может быть именем файла, не являющегося каталогом.

Каталоги (справочники) являются файлами, из которых строится иерархическая структура файловой системы. Они играют важную роль в превращении имени файла в номер индекса. Каталог — это файл,

содержимым которого является набор записей, состоящих из номера индекса и имени файла, включенного в каталог. Имя корневого каталога — /.

Содержимое файла меняется только тогда, когда в файл производится запись. Содержимое индекса меняется при изменении как содержимого файла, так и владельца файла, прав доступа и т. д. Изменение содержимого файла автоматически вызывает коррекцию индекса, однако коррекция индекса еще не означает изменение содержимого файла.

При открытии файла индекс копируется в память и записывается обратно на диск, когда последний процесс, использующий этот файл, закроет его. Многие поля в копии индекса, с которой ядро работает в памяти, аналогичны полям в заголовке буфера, и управление индексами похоже на управление буферами.

Каждому зарегистрированному пользователю соответствует некоторый каталог файловой системы, который называется домашним (home) каталогом пользователя. При входе в систему пользователь получает неограниченный доступ к своему домашнему каталогу и всем каталогам и файлам, содержащимся в нем. Пользователь может создавать, удалять и модифицировать каталоги и файлы, содержащиеся в домашнем каталоге. Потенциально возможен доступ и ко всем другим файлам, однако он может быть ограничен, если пользователь не имеет достаточных привилегий.

Поскольку ОС UNIX с самого своего зарождения задумывалась как многопользовательская операционная система, в ней всегда была актуальна проблема авторизации доступа различных пользователей к файлам файловой системы.

Под авторизацией доступа понимают действия системы, которые допускают или не допускают доступ данного пользователя к данному файлу в зависимости от прав доступа пользователя и ограничений доступа, установленных для файла.

Схема авторизации доступа, примененная в ОС UNIX, настолько проста и удобна и одновременно настолько мощна, что стала фактическим стандартом многих современных операционных систем.

С каждым выполняемым процессом в ОС UNIX связываются реальный идентификатор пользователя (real user ID), действующий идентификатор пользователя (effective user ID) и сохраненный идентификатор пользователя (saved user ID). Все эти идентификаторы устанавливаются с помощью системного вызова `setuid`, который можно выполнять только в режиме суперпользователя.

Аналогично, с каждым процессом связываются три идентификатора группы пользователей — real group ID, effective group ID и saved group ID. Эти идентификаторы устанавливаются привилегированным системным вызовом `setgid`.

При входе пользователя в систему программа login проверяет, что пользователь зарегистрирован в системе и знает правильный пароль (если он установлен), образует новый процесс и запускает в нем требуемую для данного пользователя оболочку. Но перед этим login уста-

навливает для вновь созданного процесса идентификаторы пользователя и группы, используя для этого информацию, хранящуюся в файлах /etc/passwd и /etc/group.

После того как с процессом будут связаны идентификаторы пользователя и группы, для этого процесса начинают действовать ограничения для доступа к файлам. Процесс может получить доступ к файлу или выполнить его (если файл содержит выполняемую программу) только в том случае, если установленные для файла ограничения доступа позволяют это сделать. Связанные с процессом идентификаторы передаются создаваемым им процессам, распространяя на них те же ограничения. Однако в некоторых случаях процесс может изменить свои права с помощью системных вызовов `setuid` и `setgid`, а иногда система может изменить права доступа процесса автоматически.

Рассмотрим, например, следующую ситуацию. В файл /etc/passwd запрещена запись всем, кроме суперпользователя (суперпользователь может писать в любой файл). Этот файл, помимо прочего, содержит пароли пользователей, и каждому пользователю разрешается изменять свой пароль. Имеется специальная программа /bin/passwd, изменяющая пароли. Однако пользователь не может сделать это даже с помощью этой программы, поскольку запись в файл /etc/passwd запрещена.

В системе UNIX эта проблема разрешается следующим образом. Для выполняемого файла может быть указано, что при его запуске должны устанавливаться идентификаторы пользователя и/или группы. Если пользователь запрашивает выполнение такой программы (с помощью системного вызова `exec`), то для этого процесса устанавливаются идентификатор пользователя, соответствующий идентификатору владельца выполняемого файла, и/или идентификатор группы этого владельца. В частности, при запуске программы /bin/passwd процесс получит идентификатор суперпользователя и программа сможет произвести запись в файл /etc/passwd.

Как для идентификатора пользователя, так и для идентификатора группы реальный ID является истинным идентификатором, а действующий ID — идентификатором текущего выполнения. Если текущий идентификатор пользователя соответствует суперпользователю, то этот идентификатор и идентификатор группы могут быть переназначены в любое значение системными вызовами `setuid` и `setgid`. Если же текущий идентификатор пользователя отличается от идентификатора суперпользователя, то выполнение системных вызовов `setuid` и `setgid` приводит к замене текущего идентификатора истинным идентификатором (пользователя или группы соответственно).

Как обычно принято в многопользовательской операционной системе, в UNIX поддерживается единообразный механизм контроля доступа к файлам и справочникам файловой системы. Любой процесс может получить доступ к некоторому файлу в том и только в том случае, если права доступа, описанные при файле, соответствуют возможностям данного процесса.

Традиционно в файловых системах ОС UNIX за доступ ко всем типам файлов (файлы, справочники и специальные файлы) отвечают 9 бит, которые хранятся в i-узле. Первая группа из 3 битов определяет права доступа к файлу для его владельца, вторая — для членов группы владельца, третья — для всех остальных пользователей.

Например, права доступа `rwxr-xr-` к файлу означают, что владелец файла имеет полный доступ, члены группы имеют возможность чтения и выполнения, все остальные могут только читать данный файл. Для справочника установка бита выполнения `x` означает возможность поиска (извлечения) файлов из этого справочника.

Согласно принципам построения ОС UNIX необходим еще четвертый бит, определяющий права на выполнение исполняемого файла. Четвертый бит в самом общем случае интерпретируется как возможность смены идентификатора пользователя. Его смысловая нагрузка меняется в зависимости от того, в какой группе битов доступа он установлен.

Защита файлов от несанкционированного доступа в ОС UNIX основывается на трех факторах:

1. С любым процессом, создающим файл (или справочник), ассоциирован некоторый уникальный в системе идентификатор пользователя (UID — User Identifier), который в дальнейшем можно трактовать как идентификатор владельца вновь созданного файла.

2. С каждый процессом, пытающимся получить некоторый доступ к файлу, связана пара идентификаторов — текущие идентификаторы пользователя и его группы.

3. Каждому файлу однозначно соответствует его описатель — i-узел.

На последнем факторе следует остановиться более подробно. Важно понимать, что имена файлов и файлы как таковые — это не одно и то же. В частности, при наличии нескольких жестких связей с одним файлом несколько имен файла реально представляют один и тот же файл и ассоциированы с одним и тем же i-узлом. Любому используемому в файловой системе i-узлу всегда однозначно соответствует один и только один файл. i-узел содержит достаточно много разнообразной информации (большая ее часть доступна пользователям через системные вызовы `stat` и `fstat`), и среди этой информации находится часть, позволяющая файловой системе оценить правомочность доступа данного процесса к данному файлу в требуемом режиме.

Общие принципы защиты одинаковы для всех существующих вариантов системы. Информация i-узла включает UID и GID текущего владельца файла (немедленно после создания файла идентификаторы его текущего владельца устанавливаются соответствующим действующим идентификатором процесса-создателя, но в дальнейшем они могут быть изменены системными вызовами `chown` и `chgrp`). Кроме того, в i-узле файла хранится шкала, в которой отмечено, что может делать с файлом пользователь, являющийся его владельцем, что могут делать с файлом пользователи, входящие в ту же группу пользователей, что и владелец, и что могут делать с файлом остальные пользователи [89].

Такая система защиты файлов существует достаточно давно и не вызывает нареканий. Действительно, для того чтобы вручную, т. е. не используя системные вызовы и команды, изменить права доступа к файлу, следует иметь доступ к области i-узлов. Для того чтобы иметь доступ к области i-узлов, следует изменить права доступа специального файла (например, /dev/root), биты доступа которого также хранятся в области i-узлов. Иными словами, если случайно или умышленно не испортить права доступа ко всем файлам системы, установленные по умолчанию (обычно правильно) при инсталляции, то можно с большой степенью вероятности гарантировать безопасность работы системы.

В разных версиях системы UNIX имеются небольшие различия в реализации защиты файлов от несанкционированного доступа. Для примера приведем представление информации, ограничивающей доступ к файлу, в i-узле файла в UNIX System V Release 4 (табл. 8.3).

Таблица 8.3. **Представление информации, ограничивающей доступ к файлу, в i-узле файла**

Шкала ограничений в восьмеричном виде	Описание
04000	Установка идентификатора пользователя-владельца при выполнении файла
020n0	При n = 7, 5, 3 или 1 установка идентификатора группы владельца при выполнении файла. При n = 6, 4, 2 или 0 разрешается блокирование диапазонов адресов файла
01000	Сохранение в области подкачки образ кодового сегмента выполняемого файла после окончания его выполнения
00400	Владельцу файла разрешено чтение файла
00200	Владелец файла может дополнять или модифицировать файл
00100	Владелец файла может его исполнять, если он исполняемый, или производить в нем поиск, если это файл-каталог
00040	Все пользователи группы владельца могут читать файл
00020	Все пользователи группы владельца могут дополнять или модифицировать файл
00010	Все пользователи группы владельца могут исполнять файл, если он исполняемый, или производить в нем поиск, если это файл-каталог
00004	Все пользователи могут читать файл
00002	Все пользователи могут дополнять или модифицировать файл
00001	Все пользователи могут исполнять файл, если он исполняемый, или производить в нем поиск, если это файл-каталог

Некоторые системы UNIX (например, Solaris) предоставляют дополнительные возможности по управлению правами доступа к файлам путем использования списков управления доступом (Access Control List). Данный механизм позволяет для каждого пользователя или для

отдельной группы установить индивидуальные права доступа к заданному файлу. При этом списки доступа сохраняются всеми системными средствами копирования и архивирования. Введение этого механизма вносит определенную гибкость в процедуру формирования прав доступа к файлам.

8.3.4. Средства аудита

В ОС UNIX имеются инструменты системного *аудита*, осуществляющие хронологическую запись событий, имеющих отношение к безопасности. К таким событиям обычно относят: обращения программ к отдельным серверам; события, связанные с входом в систему/выходом из нее и др. Обычно регистрационные действия выполняются специализированным syslog-демоном, который проводит запись событий в регистрационный журнал в соответствии с текущей конфигурацией. Syslog-демон стартует в процессе загрузки системы.

Система контроля регистрирует события в операционной системе, связанные с защитой информации, записывая их в контрольный журнал. В контрольных журналах возможна фиксация случаев проникновения в систему и неправильного использования ресурсов.

Контроль позволяет просматривать собранные данные для изучения видов доступа к объектам и наблюдения за действиями отдельных пользователей и их процессов. Попытки нарушения защиты и механизмов авторизации контролируются. Использование системы контроля дает высокую степень гарантии обнаружения попыток обойти механизмы обеспечения безопасности. Поскольку события, связанные с защитой информации, контролируются и учитываются вплоть до выявления конкретного пользователя, система контроля служит сдерживающим средством для пользователей, пытающихся некорректно использовать систему.

В соответствии с требованиями по надежности операционная система должна создавать, поддерживать и защищать журнал регистрационной информации, относящейся к доступу к объектам, которые контролируются системой. При этом должна быть возможность регистрации следующих событий:

- использования механизма идентификации и аутентификации;
- внесения объектов в адресное пространство пользователя (например, открытия файла);
- удаления объектов;
- действий администраторов;
- других событий, затрагивающих информационную безопасность.

Каждая регистрационная запись должна включать следующие поля:

- даты и времени события;
- идентификатора пользователя;
- типа события;
- результата действия.

Для событий идентификации и аутентификации регистрируется также идентификатор устройства. Для действий с объектами регистрируются имена объектов.

Типы контролируемых событий, поддерживаемые в SCO UNIX Release 5.0, приведены в табл. 8.4.

Таблица 8.4. **Типы контролируемых событий, поддерживаемые в SCO Release 5.0**

Тип контролируемого события	Описание
Startup/Shutdown	Старт (загрузка)/выгрузка системы
Login/Logout	Успешный вход и выход из системы
Process Create/Delete	Создание/уничтожение процесса
Make Object Available	Сделать объект доступным (открыть файл, открыть сообщения, открыть семафор, монтировать файловую систему и т. п.)
Map Object to Subject	Отобразить объект в субъект (выполнение программы)
Object Modification	Модификация объекта (запись в файл и т. п.)
Make Object Unavailable	Сделать объект недоступным (закрыть файл, закрыть сообщение, закрыть семафор, размонтировать файловую систему и т. п.)
Object Creation	Создание объекта (создание файла/сообщения/семафора и т. п.)
Object Deletion	Удаление объекта (удаление файла/сообщения/семафора и т. п.)
DAC Changes	Изменение разграничения доступа (изменение доступа к файлу, сообщению, семафору, изменение владельца и т. п.)
DAC Denials	Отказ доступа (отсутствие прав доступа к какому-либо объекту)
Admin/Operator Actions	Действия (команды) системных администраторов и операторов
Insufficient Authorization	Процессы, которые пытаются превысить свои полномочия
Resource Denials	Отказы в ресурсах (отсутствие необходимых файлов, превышение объема памяти и т. п.)
IPC Functions	Посылка сигналов и сообщений процессам
Process Modifications	Модификации процесса (изменение эффективного идентификатора процесса, текущего справочника процесса и т. п.)
Audit Subsystem Events	События системы контроля (разрешение/запрещение системного контроля и модификация событий контроля)
Database Events	События базы данных (изменение данных безопасности системы и их целостности)
Subsystem Events	События подсистемы (использование защищенных подсистем)
Use of Authorization	Использование привилегий (контроль действий с использованием различных привилегий)

Система контроля использует системные вызовы и утилиты для классификации действий пользователей, подразделяя их на события различного типа. Например, при возникновении события типа DAC Denials (отказ в доступе при реализации механизма избирательного разграничения доступа) регистрируются попытки такого использования объекта, которые не допускаются разрешениями для этого объекта. Например, если пользовательский процесс пытается писать в файл с доступом только для чтения, то возникает событие типа DAC Denials. Если просмотреть контрольный журнал, то легко можно увидеть повторяющиеся попытки доступа к файлам, на которые не получены разрешения.

Существенно повышает эффективность контроля наличие регистрационного идентификатора пользователя (LUID). После прохождения пользователем процедур идентификации и аутентификации, т. е. непосредственного входа в систему, каждому процессу, создаваемому пользователем, присваивается регистрационный идентификатор пользователя. Данный идентификатор сохраняется с помощью таких команд, как `su`.

Каждая контрольная запись, генерируемая системой контроля, содержит для каждого процесса регистрационный идентификатор наряду с эффективным и реальным идентификаторами пользователя и группы. Таким образом, оказывается возможным выполнять учет действий пользователя.

Отдельно следует рассмотреть реализацию механизма контроля для работы в режиме ядра. Данный механизм генерирует контрольные записи по результатам выполнения пользовательских процессов с помощью системных вызовов ядра. Каждый системный вызов ядра содержит строку в таблице, в которой указывается связь системного вызова с контролем защиты информации и тип события, которому он соответствует.

Кроме того, используется таблица кодов ошибок, позволяющая классифицировать системные вызовы как конкретные события, связанные с защитой информации.

Например, системный вызов `open` классифицируется как событие Make Object Available. Если пользователь выполняет системный вызов `open` для файла /unix и данный системный вызов завершается успешно, то генерируется контрольная запись об этом событии. Однако если системный вызов `open` заканчивается неудачно в силу того, что пользователь запросил в системном вызове доступ на запись файла /unix, не имея разрешения, то это действие классифицируется как событие DAC Denials для данного пользователя и объекта /unix. Следовательно, системный вызов можно отобразить в несколько типов событий, в зависимости от объекта, к которому осуществляется доступ, и результата вызова.

Некоторые системные вызовы не имеют отношения к защите информации. Например, системный вызов `getpid` получает идентификатор процесса и не определяет никакого события, связанного с защитой

информации. Таким образом, данный системный вызов не подлежит контролю.

Механизм контроля ядра выдает внутренний вызов в драйвер устройства для занесения записи в контрольный журнал. Отметим, что информацию контроля система записывает непосредственно на диск, не дожидаясь синхронизации суперблоков в оперативной памяти и на диске. Этим достигается полная защита от разрушения информации контроля.

Однако следует иметь в виду, что при включении всех событий контроля и при активной работе пользователей объем записываемой информации может достигать нескольких мегабайтов на одного пользователя в час. Поэтому контроль следует рассматривать не как превентивную меру, а как меру пресечения.

8.3.5. Безопасность системы UNIX при работе в сети

В сегодняшних условиях особую актуальность имеют вопросы безопасности систем UNIX при работе в сети. По историческим причинам (из-за давности разработки базовых средств сетевого обмена, используемых в UNIX) при построении сетей UNIX возникают серьезные проблемы безопасности. Сетевая файловая система NFS (Network File System) предназначена для прозрачного доступа пользователей к файловым системам компьютеров UNIX по сети. Существенным недостатком NFS с точки зрения безопасности является возможность администратора предоставить доступ по сети к любому справочнику файловой системы независимо от его владельца. Никем не контролируемое чтение экспортированных справочников любым пользователем сети является серьезным недостатком при построении безопасных систем.

При построении защиты информации на уровне сети существуют свои особенности.

Во-первых, из-за возможности перехвата пакетов и передачи отдельными видами сервисов паролей в открытом виде существует необходимость дополнительной аутентификации пользователей. Во-вторых, возникает необходимость аутентификации удаленных машин. В-третьих, необходимы дополнительные средства контроля событий, которые возникают при работе на сетевом уровне.

Отметим, что на сетевом уровне системы UNIX не обладают столь мощными стандартными средствами обеспечения безопасности, как на системном. Слабость защиты на уровне сети может свести к нулю все результаты защиты базовой системы. Поэтому для обеспечения безопасности систем UNIX при работе в сети требуются дополнительные средства защиты.

Защита на сетевом уровне требует использования некоторых дополнительных стандартных средств и методов. Прежде всего это сис-

тема аутентификации Kerberos и межсетевые экраны (Firewall). Заметим, что некоторые системы UNIX включают в качестве стандартных средств защиты, например, клиента системы Kerberos. Решение проблемы закрытия сетевого трафика должно быть сделано на уровне не ОС, а единого стандарта, например протокола IPSec. Перечисленные методы и средства будут подробно рассмотрены в последующих главах.

8.4. Безопасность ОС Windows Vista

Корпорация Майкрософт объявила о создании операционной системы Windows Vista в конце 2006 г. В операционной системе Windows Vista с самого начала были заложены принципы комплексного обеспечения безопасности.

Корпорация Microsoft предлагает несколько вариантов операционной системы Microsoft Windows Vista, каждый из которых ориентирован на удовлетворение потребностей отдельной категории клиентов.

Для каждого из основных сегментов рынка — домашних пользователей, малых, средних и крупных предприятий — корпорация Майкрософт предлагает по меньшей мере один базовый и один расширенный выпуск.

Windows Vista Home Basic является базовым выпуском для домашних пользователей.

Windows Vista Home Premium является выпуском с расширенным набором возможностей для домашних пользователей.

Windows Vista Business является базовым выпуском для организаций любых размеров.

Windows Vista Enterprise — расширенный выпуск операционной системы для предприятий. Особое внимание в нем уделено удовлетворению потребностей организаций с глобальной и крайне сложной ИТ-инфраструктурой.

Windows Vista Ultimate является выпуском для наиболее требовательных потребителей, желающих воспользоваться всеми преимуществами Windows Vista. Он включает в себя все функции операционных систем Windows Vista для всех потребительских сегментов рынка.

В Windows Vista реализована многоступенчатая защита: даже если злоумышленнику удастся попасть в систему, он натолкнется на множество механизмов обеспечения безопасности, которые не дадут ему предпринять какие-либо действия.

При разработке операционной системы Windows Vista использовались передовые технологии безопасности, в частности впервые примененные в пакете обновления 2 (SP2) для Windows XP. В Windows Vista включено много новых функций, обеспечивающих безопасность, и прочих улучшений, направленных на защиту компьютеров пользователей от всевозможных угроз последнего поколения, в том числе вирусов,

червей и вредоносного программного обеспечения. Рассмотрим основные функции и средства защиты, обеспечивающие безопасность операционной системы Windows Vista [23, 91, 99].

8.4.1. Средства защиты общего характера

Рассмотрим входящие в состав Windows Vista средства защиты общего характера:

- поддержка аппаратных средств защиты;
- защита драйверов;
- защита от атак на системные службы;
- защита доступа к сети;
- управление учетными записями пользователей.

Поддержка аппаратных средств защиты

В первую очередь следует отметить случайное расположение адресного пространства (Address Space Layout Randomization — ASLR). Суть этого вида защиты заключается в случайном выборе адресов памяти для расположения ключевых системных исполняемых файлов и библиотек при перезагрузке системы, что осложняет вредоносному программному обеспечению поиск файлов, которые оно использует для атаки.

Еще один вид защиты в Windows Vista, затрудняющий применение системных функций вредоносным кодом, — это Data Execution Prevention, т. е. поддержка реализованной на уровне процессора технологии NX (No eXecute), которая дает программному обеспечению возможность помечать сегменты памяти, где могут храниться только данные, и тем самым не разрешать приложениям исполнять произвольный код в таких сегментах (это могут делать многие современные процессоры). Поддержка технологии NX позволяет исключить выполнение кода в областях памяти, предназначенных для хранения данных, что нередко используется вредоносным ПО для получения возможности управлять компьютером. Кроме того, разработчики приложений для данной операционной системы могут встраивать поддержку технологии NX в свои продукты — для этого им предоставляется соответствующий программный интерфейс.

Из улучшений в области поддержки аппаратных средств защиты отметим механизмы определения переполнения «кучи» (области памяти, выделяемой программе для динамически размещаемых структур данных), позволяющие операционной системе немедленно завершить выполнение приложения, в котором произошло переполнение. Переполнение «кучи» нередко применяется вредоносным кодом. Определение переполнения «кучи» может быть использовано и независимыми разработчиками — эта функциональность поддерживается в Windows API.

В дополнение к вышеперечисленным технологиям поддержки аппаратных средств защиты 64-разрядные версии Windows Vista поддер-

живают технологию защиты ядра операционной системы PatchGuard, запрещающую внесение изменений в ядро операционной системы (а именно в таблицы системных вызовов, прерываний, глобальных дескрипторов). Отметим, что в предыдущих версиях Windows технологии модификации ядра ОС применялись некоторыми независимыми производителями ПО и, соответственно, могли использоваться и авторами вредоносного кода. Согласно заявлению «Майкрософт», отключить систему защиты ядра невозможно — кроме официальных обновлений самой «Майкрософт», вносить изменения в ядро ОС не может никакое программное обеспечение. Впрочем, в 32-разрядных версиях Windows Vista защиты ядра нет.

Защита драйверов

Механизм проверки цифровой подписи драйверов присутствует во всех версиях Windows, начиная с Windows 2000. Однако реально средства запрета установки драйверов, не имеющих цифровой подписи, не применялись ни пользователями, ни системными администраторами — ведь неподписанных драйверов, не содержащих вредоносного кода, существует великое множество.

Теперь же все драйверы, предназначенные для 64-разрядных версий Windows Vista, должны иметь цифровую подпись — в противном случае они просто не будут загружены. Это позволяет предотвратить ряд атак, основанных на модификации или имитации драйверов. Отметим, что данная мера дает возможность повысить не только защищенность, но и надежность операционной системы, позволяя идентифицировать источник ее сбоев. Впрочем, в некоторых случаях это может усложнить поиск или написание нужного драйвера.

Защита от атак на системные службы

Системные службы, выполняемые с самыми высокими привилегиями, являются излюбленной мишенью для атак злоумышленников, поскольку скомпрометированная системная служба может позволить исполнить произвольный код с административными полномочиями. Поэтому защита от атак на системные службы (Windows Service Hardening) является важной составляющей защиты операционной системы.

Для снижения вероятности успешных атак на системные службы в Windows Vista реализована концепция *restricted services*, заключающаяся в загрузке системных служб с минимальными привилегиями. Данный подход позволяет существенно сократить число служб, способных нанести серьезный вред операционной системе. Кроме того, можно однозначно идентифицировать системные службы, вести списки контроля доступа для каждой службы к реестру, файловой системе, сетевым портам или к другим системным ресурсам и предотвращать их изменение скомпрометированными службами. Более того, каждая служба имеет

свой заранее сконфигурированный профиль, который учитывает требования безопасности и применяется при установке операционной системы, что позволяет упростить процесс первоначального конфигурирования служб.

Отметим, что персональный межсетевой экран Windows Firewall в Windows Vista тоже обеспечивает защиту от атак на системные службы. Так, он блокирует попытки обращения системных служб к сетевым портам и к другим ресурсам, которые запрещено применять данной службе.

Защита доступа к сети

В состав Windows Vista включен агент, который может предоставить информацию о статусе работоспособного состояния клиентов сети и о настройках доступа к серверам и узлам сети. Клиенты, которые не имеют последних обновлений безопасности, антивирусных программ или другим образом не удовлетворяют необходимым требованиям, определяющим понятие «работоспособное состояние», не могут работать в вашей сети. Защита доступа к сети (Network Access Protection) может использоваться для того, чтобы защитить вашу сеть как от удаленных клиентов, так и от клиентов локальной сети (LAN), использующих проводное или беспроводное подключение. Агент проверяет такие аспекты работоспособности клиента Windows Vista, как наличие последних обновлений и свежих антивирусных баз, и сообщает о них службе усиления защиты доступа к сети (Network Access Protection Enforcement Service), базирующейся на архитектуре сети с выделенным сервером. Система защиты доступа к сети, включенная в Windows Server «Longhorn», решает, предоставить ли клиенту доступ к сети.

Управление учетными записями пользователей

Набор функций Windows Vista для управления учетной записью пользователя (User Account Control — UAC) помогает соблюсти баланс между гибкими и богатыми возможностями учетной записи администратора и обеспечением безопасности стандартной учетной записи пользователя.

Наличие избыточных привилегий у пользовательских учетных записей считается одной из самых серьезных угроз безопасности в Windows XP. Предоставление пользователям административных привилегий нередко было вынужденной мерой, необходимой для нормальной повседневной работы пользователей. Однако подобный подход снижал степень защищенности компьютера, позволяя выполнять с административными привилегиями не только системные утилиты и бизнес-приложения, но и вредоносный код, который, в свою очередь, мог вносить изменения в конфигурацию компьютера или отключать брандмауэр. Кроме того, вероятность ошибок пользователей, услож-

няющих сопровождение рабочих станций и сетей, тоже была довольно велика.

Отметим, что доступная в прежних версиях Windows возможность создания учетных записей с ограниченными правами на практике использовалась редко, так как она усложняла работу и пользователю, и системному администратору — ведь любая простейшая манипуляция наподобие установки драйвера принтера требовала административных привилегий.

Для решения этой проблемы в Windows Vista применяется технология управления учетными записями пользователей UAC (User Account Control). В ее основе лежит деление манипуляций с настройками операционной системы на доступные пользователю со стандартными правами (т. е. не создающие непосредственной угрозы безопасности компьютера и сети) и требующие административных привилегий.

К первой группе относятся такие функции, как изменение настроек управления питанием, добавление устройств, драйверы которых уже установлены в операционной системе, изменение настроек экрана, добавление шрифтов, создание VPN-соединений и соединений с беспроводными сетями, установка UAC-совместимых обновлений ПО, т. е. функции, повседневно применяемые пользователями. Технология управления учетными записями пользователей UAC позволяет обычным пользователям работать, оставаясь в рамках стандартных привилегий.

Ко второй группе принадлежат задачи, требующие административных привилегий, такие как установка новых приложений, изменение системных настроек, добавление новых драйверов устройств. Когда пользователь пытается выполнить подобную задачу, ему предлагается ввести пароль администратора. При этом системные администраторы могут отключить процедуру ввода пароля администратора для обычных пользователей, сокращая риск несанкционированных действий со стороны последних.

Пользователи с административными привилегиями могут работать в режиме ограничения доступа к критичным ресурсам и функциям системы до тех пор, пока этот доступ им реально не потребуется. Пользовательский интерфейс Windows Vista включает ряд средств, упрощающих выявление задач, которые требуют административных привилегий. Так, на кнопке, по которой следует щелкнуть для выполнения подобного действия, отображается специальный значок и описание этого действия.

Для обеспечения совместимости с уже существующими приложениями технология UAC позволяет приложениям, созданным для прежних версий Windows и требующим административных привилегий, выполняться с правами стандартного пользователя за счет предоставления для них механизма виртуализации файловой системы и реестра. Данный механизм перенаправляет запросы чтения и записи из защищенных областей памяти и реестра в выделенную область внутри профиля пользователя, не влияя ни на настройки и данные других пользователей, ни на конфигурацию операционной системы. Хотя подобный ме-

ханизм и исключает доступ приложений к критически важным ресурсам, компания «Майкрософт» рекомендует использовать его только как временную меру, до момента создания новых версий подобных приложений, не требующих административных привилегий и поддерживающих UAC.

Средства UAC также помогают защитить домашние компьютеры от вредоносных программ. Часто вредоносные коды скрыты в программах, привлекательных для детей. Чтобы защитить компьютер, можно создать для детей стандартные учетные записи пользователей. В этом случае, если ребенок попытается установить программное обеспечение, будет выдан запрос пароля учетной записи администратора. Дети не смогут самостоятельно устанавливать новые программы.

8.4.2. Защита от вредоносных программ

Вредоносные программы, такие как вирусы, компьютерные черви, шпионские программы и другое нежелательное программное обеспечение, могут вызывать самые разные проблемы, в том числе кражу личных сведений, замедление работы компьютера и компьютерной сети в целом, появление нежелательной рекламы (например, всплывающих окон с рекламой). Более того, некоторые программы осуществляют незаконный сбор как бизнес-информации, хранимой на компьютерах пользователей и на сервере, так и конфиденциальных личных данных.

В соответствии с концепцией «Майкрософт» о многоуровневой защите в составе Windows Vista реализованы новые функции, которые предотвращают установку вредоносных программ на компьютер, помогают уменьшить ущерб, наносимый такими программами, если им все же удалось проникнуть в систему, и удаляют уже установленные вредоносные программы.

Для защиты от вредоносных программ в составе Windows Vista имеются следующие средства:

- межсетевой экран Windows Firewall;
- Центр безопасности Windows;
- управление учетными записями пользователей;
- защищенный режим Internet Explorer 7;
- Защитник Windows.

При использовании с другими приложениями и службами «Майкрософт», такими как средство удаления вредоносных программ для Windows, и антивирусным программным обеспечением любого из партнеров компании «Майкрософт» операционная система Windows Vista гарантирует надежную защиту компьютера от вредоносных программ.

Управление учетными записями пользователей было рассмотрено в предыдущем разделе. Защищенный режим Internet Explorer 7 описан ниже в разделе «Безопасность Internet Explorer 7». Рассмотрим остальные функции, используемые для защиты от вредоносных программ в составе Windows Vista.

Межсетевой экран Windows Firewall

Межсетевой экран Windows Firewall служит первой линией защиты от различного рода вредоносных программ. Начиная с версии Windows XP Service Pack 2, межсетевой экран Windows Firewall включен по умолчанию и защищает компьютер с момента загрузки операционной системы. Он удобен в использовании, легко настраивается, имеет простой интерфейс и практически незаметен при работе. Если в операционной системе Windows XP Service Pack 2 межсетевой экран фильтрует только входящий трафик, то в Windows Vista межсетевой экран является двусторонним, позволяя осуществлять фильтрацию как входящего, так и исходящего трафика. Межсетевой экран Windows Firewall может блокировать весь входящий трафик до тех пор, пока на компьютер не будут установлены все последние пакеты обновлений.

Межсетевой экран Windows Firewall постоянно следит за ресурсами операционной системы и, если они начинают вести себя неожиданным образом, что обычно указывает на присутствие вредоносных программ, выполняет защитные действия. Например, если компонент Windows, который должен отправлять сетевые сообщения через определенный порт компьютера, в результате заражения системы вирусом или червем пытается сделать это через другой порт, то межсетевой экран Windows Firewall не позволит сообщению покинуть компьютер, предотвращая тем самым проникновение вредоносной программы в другие системы локальной сети.

Всеми параметрами межсетевого экрана Windows Firewall можно управлять централизованно через групповые политики (Group Policy), тем самым обеспечивая неизменность настроек безопасности клиента. Панель управления межсетевого экрана Windows Firewall удобна в использовании, имеет простой интерфейс и всего несколько параметров настройки.

Впервые в семействе операционных систем Windows управление межсетевым экраном Windows Firewall объединено с IPsec. Межсетевой экран работает в тесном взаимодействии со службой Windows Service Hardening, позволяя ограничить возможные действия служб в системе, обеспечивая всестороннюю защиту и снижая вероятность поставить под угрозу безопасность компьютера для атакующих злоумышленников, использующих найденные уязвимости. Служба Windows Service Hardening ограничивает важные службы Windows от несвойственных им действий в файловой системе, реестре, сети или любых других местах, которые может использовать вредоносное программное обеспечение (malware) для своей установки или атаки на другие компьютеры. Например, можно ограничить службу удаленного вызова процедур RPC (Remote Procedure Call), запретив ей производить замену системных файлов или вносить изменения в реестр.

При надлежащей настройке межсетевой экран Windows Firewall не позволяет большинству вредоносных программ проникать в систему,

обеспечивая защиту от хакеров, вирусов и компьютерных червей, которые пытаются получить доступ к компьютеру через Интернет.

Центр безопасности Windows

Центр безопасности Windows WSC (Windows Security Center) позволяет автоматически загружать и устанавливать на компьютер последние обновления системы безопасности и функциональные обновления.

Центр безопасности Windows WSC (он появился в пакете обновлений Windows XP Service Pack 2) является компонентом операционной системы, постоянно проверяющим состояние межсетевого экрана, антивирусного ПО и обновлений ОС. В Windows Vista он претерпел ряд изменений. Так, в дополнение к имевшейся ранее функциональности Центр безопасности WSC отслеживает состояние настроек защиты Internet Explorer и UAC, состояние защитного ПО независимых производителей и наличие в параметрах безопасности потенциально уязвимых мест, которые следует устранить.

В Центре безопасности Windows может отображаться состояние параметров межсетевого экрана и сведения о том, настроен ли компьютер на автоматический прием обновлений от корпорации «Майкрософт». Кроме того, этот компонент осуществляет мониторинг приложений для защиты от вирусов и шпионских программ, оповещая пользователя, если такие приложения отсутствуют или требуют обновления. Проверяются также параметры безопасности Internet Explorer и функции контроля учетных записей пользователей. Если они являются недостаточно надежными, Центр безопасности Windows сообщает об этом пользователю и предоставляет рекомендации по устранению проблемы. Процесс обновления происходит в фоновом режиме, незаметно для пользователя, а перезагрузку системы можно отложить до более удобного времени.

Защищенный режим Internet Explorer 7

Веб-браузеры очень часто становятся объектом злоумышленных атак, направленных на внедрение вредоносного программного обеспечения или причинение другого вреда чужим компьютерам. В системе безопасности Internet Explorer 7 в Windows Vista реализован ряд усовершенствований, помогающих обезопасить пользователя от подобных атак (см. раздел «Безопасность Internet Explorer 7» ниже).

Защитник Windows

Защитник Windows (Windows Defender; прежнее название — Windows AntiSpyware) — это компонент Windows Vista, который регулярно проверяет жесткий диск на наличие нежелательных приложений,

контролирует системные папки, отслеживая изменения, свидетельствующие о присутствии шпионских программ, и сравнивая все файлы, к которым был получен доступ, с постоянно обновляемой базой известных шпионских программ.

При этом важно отметить, что в Windows Vista нет средств для обеспечения защиты в режиме реального времени (в момент доступа). Описанные выше функции дополняют, но не заменяют антивирусное программное обеспечение, разрабатываемое сторонними компаниями. То есть для полноценной защиты новой операционной системы необходимо дополнительно установить антивирусное ПО. Более того, если оно не установлено, то выдается соответствующее окно-предупреждение.

Таким образом, Защитник Windows хотя и позиционируется как средство защиты от шпионского и другого нежелательного ПО, но не может служить полноценной заменой антивирусного ПО. Кроме того, Защитник Windows представляет собой решение исключительно для персональных пользователей и не обладает возможностью удаленного управления, о чем, в частности, упомянуто на сайте Майкрософт.

Рассмотрим основные функции Защитника Windows.

Программа проста в использовании и поставляется с предварительно заданными параметрами и инструкциями по обеспечению безопасности. Она автоматически обрабатывает многие стандартные задачи и обращается к пользователю только в случае возникновения проблем, требующих его немедленного вмешательства.

Защитник Windows использует ряд усовершенствований в составе Windows Vista, включая модернизированную технологию кэширования, которая ускоряет сканирование, и функцию контроля учетных записей пользователей, позволяющую запускать приложения даже без привилегий администратора. Благодаря интеграции с Internet Explorer загружаемые из Интернета файлы проверяются до сохранения и выполнения, что снижает вероятность случайной установки шпионских программ.

В Защитнике Windows используются три технологии:

- поиск и удаление шпионских программ;
- защита в режиме реального времени;
- непрерывное обновление.

По умолчанию Защитник Windows проверяет компьютер на наличие шпионских программ каждый день в 2:00, если пользователь не установил другого расписания. Можно либо провести полное сканирование, либо проверить наиболее подверженные заражению папки (например, с объектами модуля поддержки Internet Explorer).

После завершения проверки Защитник Windows сообщает о результатах и, если на компьютере были найдены шпионские программы, предлагает выбрать одно из следующих действий:

- **Пропустить**;
- **Карантин** (запустить программу нельзя, но в случае необходимости она может быть восстановлена);
- **Удалить**;

- **Всегда разрешать** (программа больше не будет обнаруживаться подобными проверками).

Защитник Windows поддерживает поиск и удаление программного обеспечения даже в том случае, если пользователь не имеет полномочий администратора. По умолчанию обычный пользователь может удалять, изолировать и пропускать обнаруженные программы.

Для борьбы с новыми и неизвестными угрозами в состав Защитника Windows включены средства защиты в режиме реального времени. Несколько агентов безопасности контролируют важные компоненты компьютера, которые могут быть изменены шпионскими программами: папку автозагрузки, параметры конфигурации, надстройки для Internet Explorer и др. Эти компоненты являются стандартными точками проникновения шпионских программ. Обнаружив подобное изменение, Защитник Windows сообщает о нем пользователю и предоставляет ему возможность заблокировать или разрешить соответствующую операцию. Подозрительно вести себя может и легальная программа, поэтому, чтобы помочь принять в отношении нее правильное решение, Защитник Windows сообщает, сколько других пользователей (в процентах от общего числа) разрешили запуск этой программы на своих компьютерах. Эффективность борьбы со шпионскими программами зависит от актуальности базы их описания. Обновленные описания создаются аналитиками корпорации «Майкрософт».

Защитник Windows позволяет получить наглядное представление об установленных на компьютере программах и лучше управлять ими. Обнаружив подозрительную операцию неизвестной программы, приложение оповещает пользователя о потенциальной угрозе. Кроме того, в состав Защитника Windows входит ряд средств и функций, предназначенных для контроля за работой установленного программного обеспечения, разъяснения сути угроз и оповещений, а также для регистрации выполненных операций сканирования и принятых мер защиты.

8.4.3. Защита данных от утечек и компрометации

Хищение или потеря корпоративной интеллектуальной собственности вызывают все большее беспокойство в организациях. При создании Windows Vista компания «Майкрософт» уделила повышенное внимание вопросам защиты данных. Windows Vista осуществляет многоуровневую защиту данных в документах, файлах, папках и на разных уровнях оборудования.

Рассмотрим входящие в состав Windows Vista средства защиты данных от утечек и компрометации:

- шифрование жесткого диска;
- улучшения в системе шифрования файлов;
- контроль USB-устройств;
- защита пользовательских данных.

Шифрование жесткого диска

Защитить конфиденциальную информацию на диске компьютера с установленной на нем операционной системой Windows Vista можно путем полного шифрования диска с помощью технологии BitLocker Drive Encryption, что позволяет избежать компрометации данных в случае его утери или кражи. В случае если диск, защищенный с помощью технологии BitLocker, украден или утерян, приватная информация не попадет в руки злоумышленников.

Технология BitLocker требует аппаратной поддержки, предоставляемой с помощью модуля TPM (Trusted Platform Module), а именно специального чипа, предназначенного для безопасного хранения данных (рис. 8.1).

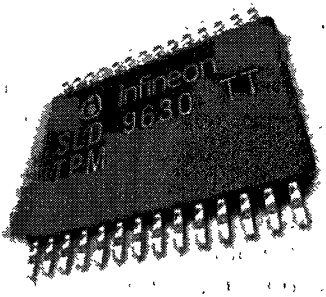


Рис. 8.1. Чип для безопасного хранения данных

Модуль TPM используется для безопасного хранения ключей шифрования и дешифрования секторов на жестком диске Windows, а также для разграничения доступа к системе. Помимо этого технология BitLocker позволяет изменить стандартный процесс загрузки операционной системы, блокируя ее, пока пользователь не вставит USB-устройство с ключами дешифрования или не введет специальный PIN-код.

Улучшения в системе шифрования файлов

Возможности системы шифрования файлов EFS (Encrypting File System) были доступны и в Windows XP. Шифрование конфиденциальных файлов средствами EFS обеспечивает их надежную защиту. Данные зашифрованного файла останутся недоступными, даже если атакующий получит полный доступ к среде хранения данных компьютера. Только полномочные пользователи и назначенные агенты восстановления данных в состоянии расшифровывать файлы. При попытке несанкционированного доступа к зашифрованному файлу система откажет в доступе.

Дополнительные функции системы шифрования файлов EFS существенно обогатили Windows Vista, обеспечив гибкость для корпоративных пользователей при развертывании решений безопасности, осно-

ванных на шифровании файлов с данными. В дополнение к функциональности, имевшейся в Windows XP, в Windows Vista система EFS поддерживает хранение пользовательских ключей и ключей восстановления на смарт-картах, обеспечивая их лучшую защиту, а также может быть использована для шифрования файла подкачки и кэша, в котором содержатся копии документов с сервера. Подобные опции, равно как и опция сохранения ключей на смарт-картах, устанавливаются в групповых политиках безопасности, что позволяет защитить документы, загружаемые с сервера, от несанкционированного доступа от имени локального администратора.

Пользователям Vista также доступна возможность шифрования пользовательских файлов «на лету» при сохранении их на сервере Longhorn.

Контроль USB-устройств

Утечка конфиденциальных данных и распространение вредоносного ПО очень часто происходят из-за бесконтрольного использования USB-накопителей. Именно поэтому в Windows Vista реализован механизм контроля применения USB-устройств. Так, системные администраторы с помощью групповых политик могут блокировать установку неавторизованных USB-устройств либо разрешить установку только определенного класса устройств, таких как принтеры, запретить установку любых типов USB-накопителей или неавторизованных устройств, устанавливать доступ к устройствам для определенных пользователей или компьютеров.

Защита пользовательских данных

В Windows Vista доступ к папке Мои документы возможен только для учетной записи пользователя, которому принадлежит данная папка, — никакие другие пользователи ни при каких условиях к ней доступа не имеют. Встроенный клиент управления правами (Rights Management) позволяет организации принудительно устанавливать политику пользования документами.

8.4.4. Безопасность Internet Explorer 7

Веб-браузеры всегда были привлекательны для злоумышленников как потенциальная брешь, открывающая доступ к ресурсам, не предназначенным для них. Поэтому защита компьютера от вредоносного ПО, использующего браузер в качестве средства проникновения в компьютер или в локальную сеть, является сегодня одной из актуальных задач.

В состав Windows Vista входит браузер Internet Explorer 7. Ниже будут рассмотрены новые функции Windows Vista и особенности функ-

ционирования этого браузера, связанные с обеспечением безопасности работы в Интернете:

- защищенный режим Internet Explorer;
- контроль над расширениями браузера;
- управление параметрами безопасности;
- технология InfoCard;
- опознание некорректных URL;
- строка состояния безопасности;
- уничтожение истории посещения сайтов;
- защита от атак с применением междоменных сценариев;
- средства опознания фишинговых сайтов.

Защищенный режим Internet Explorer 7

Защищенный режим браузера Internet Explorer 7 позволяет безопасно работать в Интернете. Этот режим доступен только для пользователей, работающих с Internet Explorer 7 в Windows Vista. Он обеспечивает повышенный уровень безопасности и защиты данных для пользователей Windows.

Защищенный режим предназначен для защиты от несанкционированного получения прав. Он обеспечивает безопасность просмотра веб-узлов, не допуская несанкционированного получения доступа злоумышленников к обозревателю и выполнения ими кода за счет использования прав администратора.

В защищенном режиме Internet Explorer 7 в Windows Vista не может изменять пользовательские или системные файлы и настройки без участия пользователя. Все взаимодействие обозревателя Internet Explorer и операционной системы происходят при помощи промежуточного процесса. Промежуточный процесс не может быть запрограммирован на выполнение действий без участия пользователя. Это уменьшает вероятность автоматической загрузки или установки нежелательных программ. Никакие действия сценария или автоматические процессы не могут загружать данные или влиять на работу системы.

При работе в защищенном режиме браузер Internet Explorer не может осуществлять запись в какие-либо ресурсы зоны локального компьютера, кроме временных файлов Интернета. Чтобы обеспечить совместимость со старыми приложениями, записываемые данные перенаправляются в область временного хранения. В защищенном режиме также обеспечивается безопасность просмотра с использованием вкладок: для содержимого, находящегося вне текущей зоны безопасности, вместо вкладок открываются новые окна.

Контроль над расширениями браузера

Начальные настройки, заданные в учетных записях пользователей системы Windows Vista, ограничивают браузер Internet Explorer, предос-

тавляя ему полномочия, которых хватает только для просмотра Web, но недостаточные, чтобы производить замену файлов пользователя или установок, заданных по умолчанию.

Расширения браузера (элементы управления ActiveX, Browser Helper Objects, дополнительные инструментальные панели для осуществления поиска или доступа к другим функциям различных сайтов) являются удобным средством добавления ему дополнительной функциональности. Но зачастую и вредоносное ПО либо реализуется в виде подобных расширений, либо использует их как способ проникновения в компьютер или в локальную сеть.

Для защиты от вредоносного ПО применяется контроль над расширениями браузера с помощью уже упомянутой технологии Windows Defender, позволяющей отключить почти все предварительно установленные элементы управления ActiveX и иные потенциально уязвимые элементы.

Управление параметрами безопасности

Для предотвращения выбора значений параметров, которые не обеспечивают надлежащего уровня безопасности, на панель информации Internet Explorer 7 выводится и постоянно отображается соответствующее предупреждение. А при изменении пользователем настроек, повышающем уязвимость браузера, в окне Security Settings соответствующие элементы управления будут выделены красным цветом. Пользователь может в любой момент восстановить параметры безопасности стандартного среднего или высокого уровня с помощью команды *Fix Settings For Me...* (Исправить параметры безопасности) на панели информации или нажав на кнопку *Reset all zones to default level* вкладки *Security* окна *Internet Options*.

Технология InfoCard

InfoCard — это кодовое название новой технологии, которая может значительно повысить безопасность в операциях электронной коммерции.

Делая покупку на сайте того или иного поставщика, клиент выбирает товар, а затем, чтобы рассчитаться за покупку, ему нужно создать учетную запись, в которой требуется указать имя пользователя, пароль и личную информацию. После того как учетная запись будет создана, нужно ввести информацию о кредитной карте. Благодаря InfoCard данная процедура упрощается.

InfoCard позволяет упорядочивать цифровые идентификационные данные, обходиться меньшим числом паролей и лучше управлять распространением своих личных данных в Интернете. При посещении веб-узла, поддерживающего эту технологию, в систему можно войти, передав элемент InfoCard вместо пароля и имени пользователя. Переда-

ча InfoCard через новый интерфейс Windows Vista осуществляется очень просто.

Элементы InfoCard более безопасны, поскольку находящиеся в них личные данные шифруются и хранятся на компьютере пользователя или поставщика надежных удостоверений (такого как банк, поставщик услуг Интернета или правительственное учреждение).

Опознание некорректных URL

С целью атаки на браузеры нередко применяются URL, содержащие нестандартные символы. Так, злоумышленники часто маскируют мошеннические web-узлы под надежные и известные путем подмены символов в URL (например, на принадлежащие другой кодовой странице). Для защиты от подобных атак код, обрабатывающий URL, учитывает практически все возможные символы, которые могут быть включены злоумышленниками в URL и доменные имена. В дополнение к внутренней поддержке международных имен доменов в адресах URL браузер Internet Explorer 7 уведомляет пользователя о тех случаях, когда символы в адресе URL не принадлежат к одному языку. Помимо этого в Internet Explorer 7 включены визуальные средства контроля URL и доменных имен. Так, в новой версии браузера невозможно вывести ни основное, ни всплывающее окно без поля, содержащего его URL.

Строка состояния безопасности

В последние годы для защиты информации пользователей стали использоваться технологии шифрования связи и протокол SSL. И все же многие пользователи продолжают чрезмерно доверять веб-узлам, которые запрашивают у них конфиденциальную информацию. С появлением значительного количества веб-узлов физических лиц и малых предприятий, продающих товары в широком диапазоне цен, пользователи стали чаще сталкиваться с неизвестными организациями, которые просят сообщить им финансовые сведения. Сочетание этих факторов создает обширное поле деятельности для злоумышленников.

Для решения этой проблемы в Internet Explorer 7 используются строка состояния безопасности Internet Explorer 7, информирующая пользователя о степени безопасности и надежности веб-узла. Новая строка состояния безопасности Internet Explorer 7 располагается рядом с адресной строкой и помогает быстро отличать подлинные веб-узлы от подозрительных и вредоносных.

Она содержит четкие и хорошо заметные подсказки, характеризующие степень безопасности и надежности веб-узла, а также предоставляет удобный доступ к сертификатам, удостоверяющим его легальность. Новая строка состояния включает также значок золотого висячего замка, с помощью которого можно определить уровень доверия и безопасности веб-узла. Кроме того, в строке состояния отображается специаль-

ная цветовая кодировка, наглядно показывающая, является ли веб-узел легальным.

Обозреватель Internet Explorer 7 изменяет цвет адресной строки на зеленый для тех веб-узлов, которые имеют новые сертификаты (высокой надежности). Зеленый цвет означает, что владелец веб-узла прошел всестороннюю проверку подлинности.

Подтверждение ActiveX

Internet Explorer предоставляет веб-разработчикам платформу ActiveX, которая позволяет значительно расширить возможности обозревателя и работы в Интернете. Некоторые разработчики вредоносных программ также выбрали эту платформу для написания приложений, ворующих информацию и повреждающих пользовательские системы. Многие из таких программ предпринимают атаки на элементы управления ActiveX, входящие в операционную систему Windows. Эти элементы управления никогда не предназначались для использования в веб-приложениях.

Обозреватель Internet Explorer 7 оснащен новым мощным механизмом обеспечения безопасности платформы ActiveX. Функция подтверждения ActiveX автоматически отключает целые классы элементов управления, которые не были явно обозначены разработчиками для использования в Интернете. Это значительно уменьшает количество возможных направлений атак злоумышленников и тем самым снижает опасность ненадлежащего использования установленных элементов управления.

Теперь на панели информации появляется запрос, прежде чем пользователь сможет воспользоваться ранее установленным элементом управления ActiveX, который еще не применялся в Интернете. С помощью этого механизма уведомления пользователь может разрешать или запрещать доступ при просмотре незнакомых веб-узлов.

Функция подтверждения ActiveX защищает пользователей от веб-узлов, пытающихся осуществлять атаки автоматически. Эта функция предотвращает несанкционированный доступ и позволяет пользователю полностью управлять процессом просмотра. Чтобы разрешить загрузку элемента управления ActiveX, достаточно щелкнуть панель информации.

Уничтожение истории посещения сайтов

Все современные браузеры позволяют осуществлять полную очистку истории посещения сайтов, кэша браузера, файлов cookie, паролей, истории вызова приложений. Однако эти процедуры обычно выполняются по отдельности, а доступ к этим функциям не всегда простой. В Internet Explorer 7 удаление всех перечисленных данных осуществля-

ется одновременно с помощью пунктов меню **Сервис ⇒ Удалить журнал обозревателя.** Это облегчает ликвидацию следов конфиденциальных данных при использовании общедоступных компьютеров, например в интернет-кафе.

Защита от атак с применением междоменных сценариев

При атаках с применением междоменных сценариев сценарий из одного домена Интернета управляет информацией другого домена. Например, пользователь может посетить вредоносную страницу, которая открывает новое окно с надежной страницей (скажем, веб-узла банка). После этого пользователь получает запрос на ввод информации о счете, которая затем извлекается злоумышленником.

Для защиты от такого вида мошенничества в браузер Internet Explorer 7 были внесены усовершенствования. Теперь он учитывает доменное имя, с которого был получен каждый сценарий, и позволяет сценарию взаимодействовать только с окнами и содержимым из того же домена. Благодаря таким междоменным барьерам информация пользователя доступна только тем узлам, которым пользователь намеревается ее предоставить.

Эта новая функция усиливает защиту от вредоносных программ за счет ограничения возможностей мошеннических веб-узлов по использованию ошибок в других узлах и загрузки нежелательного содержимого на ПК пользователя.

Средства опознания фишинговых сайтов

Организаторы фишинг-атак используют массовые рассылки электронных писем от имени популярных брендов, в которые вставляют ссылки на фальшивые сайты, являющиеся точной копией настоящих. Оказавшись на таком сайте, неопытный пользователь может сообщить преступникам ценную информацию (имя пользователя, пароль для доступа, номер своей кредитной карты и т. п.). Успеху фишинг-афер способствует низкий уровень осведомленности пользователей о правилах работы компаний, от имени которых действуют преступники. Процент потенциальных жертв фишинга среди домашних пользователей весьма велик.

Internet Explorer 7 имеет фишинг-фильтр (Fishing Filter), который позволяет пользователям просматривать интернет-страницы более безопасно, сообщая пользователю, когда веб-сайт пытается перехватить его конфиденциальную информацию. Фишинг-фильтр производит анализ содержимого веб-сайта на наличие известных признаков техники фишинга, опираясь на глобальную сеть источников данных о фишинге, с дальнейшим вынесением решения, можно ли доверять данному веб-сайту. Данные, которыми пользуется фильтр, обновляют-

ся несколько раз в час, что является важным моментом, учитывая скорость, с которой фишинг-сайты могут появляться в Сети и собирать данные пользователей.

8.4.5. Обеспечение безопасности работы в корпоративных сетях

Подключение к сети является непременным условием нормальной работы большинства пользователей. Более того, пользователи все чаще хотят иметь возможность подключения своих рабочих портативных компьютеров практически к любой общедоступной или домашней сети, где бы они ни находились.

При использовании ОС Windows Vista работа в сети стала безопаснее, сетью удобнее управлять и ее можно расширять [85].

Новая версия стека TCP/IP

В ОС Windows Vista реализована новая версия стека TCP/IP, существенным образом улучшающая несколько наиболее важных аспектов сетевой работы и позволяющая добиться повышения производительности и пропускной способности, а также имеются собственная архитектура Wi-Fi и интерфейсы API для проверки сетевых пакетов.

Для максимального использования сетевых возможностей необходима комплексная настройка конфигурационных параметров TCP/IP. В Windows Vista не приходится делать это вручную, так как система сама анализирует сетевые условия и автоматически оптимизирует сетевые параметры.

В сетях с большими потерями данных, например в беспроводных, Windows Vista способна лучше восстанавливать информацию после потери одного или нескольких пакетов. Она может динамически увеличивать или уменьшать окно TCP на прием, что позволяет использовать всю ширину канала. При передаче файлов по высокоскоростной глобальной сети с большим временем отклика или при скачивании файлов из сети Интернет заметно существенное сокращение времени передачи файлов.

В состав базового сетевого стека Windows Vista включена собственная архитектура беспроводного соединения (собственный интерфейс Wi-Fi). К числу его преимуществ можно отнести гибкое использование во многих моделях устройств различных торговых марок, схожие приемы работы с разными устройствами и более надежные драйверы беспроводных сетевых карт независимых поставщиков.

Беспроводными сетями в ОС Windows Vista можно управлять централизованно, причем соединения по таким сетям поддерживают новейшие протоколы безопасности и позволяют пользователям работать с меньшими задержками. В стеке TCP/IP нового поколения реализована

новая архитектура сетевой защиты WFP (Windows Filtering Platform) с интерфейсами API, позволяющими разработчикам программного обеспечения участвовать в процессе принятия решений о фильтрации пакетов на нескольких уровнях стека протокола TCP/IP.

Эта архитектура обеспечивает поддержку таких функций сетевого экрана нового поколения, как проверка подлинности при соединении и динамическое конфигурирование сетевого экрана при использовании приложениями интерфейса Windows Sockets API (политика, зависящая от приложения).

Обеспечение безопасности сети

При работе в сети существует ряд опасностей:

- подключение к беспроводным сетям злоумышленников, имитирующих сети общего доступа;
- подключение зараженных вирусами ПК к корпоративной сети;
- попытки злоумышленников получить доступ к закрытым для них ресурсам и т. п.

ОС Windows Vista может облегчить борьбу со всеми этими опасностями благодаря дополнительным функциям сетевой защиты, простым в настройке и всеобъемлющим одновременно.

Собственная архитектура Wi-Fi в Windows Vista имеет широкую поддержку новейших протоколов безопасности, в том числе корпоративной и персональной версии протокола WPA2 (Wi-Fi Protected Access), протоколов PEAP-TLS и PEAP-MS-CHAP v2 (защищенный наращиваемый протокол аутентификации с обеспечением безопасности на транспортном уровне и с протоколом взаимной аутентификации). Такая широкая поддержка обеспечивает возможность взаимодействия между Windows Vista и почти всеми беспроводными устройствами.

Windows Vista анализирует характеристики беспроводной сетевой карты, что позволяет по умолчанию выбрать наиболее безопасный протокол при подключении к беспроводной сети или создании такой сети.

При помощи платформы EAP-HOST ОС Windows Vista может поддерживать специализированные механизмы аутентификации, разработанные поставщиком беспроводных устройств или какой-либо организацией.

В ОС Windows Vista реализованы многочисленные усовершенствования клиентской части беспроводного соединения, позволяющие отражать ненаправленные беспроводные атаки. Такой клиент автоматически подключается только к сетям, указанным пользователем в списке разрешенных сетей, или подключается по прямому требованию пользователя. К временным сетям он автоматически не подключается. Кроме того, если пользователь собирается установить соединение с ненадежной сетью, клиент выдает предупреждение.

Собственный клиент беспроводного соединения ОС Windows Vista поддерживает функцию единого входа (SSO), осуществляющую аутентификацию пользователя в сети на уровне 2 в необходимый момент времени с учетом настроек сетевой безопасности, причем вход в сеть и вход в систему Windows при этом взаимосвязаны. После создания профиля единого входа вход в сеть будет осуществляться раньше входа в систему Windows. Эта возможность позволяет выполнять такие операции, как обновление групповой политики, запуск сценариев регистрации, начальная загрузка по беспроводной сети, требующие подключения к сети прежде входа пользователя в систему.

Сетевой экран с дополнительными функциями безопасности обеспечивает новый уровень сетевой защиты в системе Windows Vista с поддержкой фильтрации входящих и исходящих пакетов и функции повышения стойкости служб (Windows Service Hardening). Если сетевой экран обнаруживает, что поведение какой-либо службы Windows отклоняется от нормального, описанного в сетевых правилах системы повышения стойкости служб, то он блокирует эту службу.

Одно из наиболее существенных изменений в сетевом экране заключается в его объединении со службой IPSec. В Windows Vista для защиты сети от несанкционированного доступа администраторы могут создавать простые правила сетевой безопасности, объединяющие правила сетевого экрана и IPSec.

Благодаря такому объединению можно осуществлять сквозную передачу данных по сети после установления подлинности обменивающихся сторон с обеспечением расширяемого многоуровневого доступа к доверенным сетевым ресурсам и/или защиты конфиденциальности и целостности данных.

Администратор может логически разделить корпоративную сеть на зоны, доступ в которые может быть предоставлен любому компьютеру (в том числе с правами гостя) либо только компьютерам, прошедшим аутентификацию в домене (отделение домена).

Кроме того, администратор может отделить некоторые серверы, доступ к которым следует предоставлять только определенной группе пользователей или компьютеров, например сервер приложений отдела кадров с разрешением доступа только компьютерам отдела кадров (отделение сервера).

Вирусы или черви могут проникать в локальные сети через портативные компьютеры и быстро заражать другие компьютеры. При подключении компьютера с ОС Windows Vista к сети на основе сервера Windows Server под кодовым названием Longhorn поддерживается функция защиты сетевого доступа NAP, обеспечивающая снижение риска прямого подключения зараженных компьютеров к частным сетям или их подключения по туннелю VPN.

Если на компьютере с ОС Windows Vista не установлены последние обновления по безопасности, нет образов вирусов или обнаружены другие нарушения корпоративных требований по безопасности, то NAP

не предоставляет этому компьютеру полный доступ к сети. Вместо этого данный компьютер будет подключен к ограниченной сети, где на него можно скачать и установить обновления, образы вирусов или конфигурационные настройки, необходимые для соответствия действующим требованиям по защите от вирусов.

Упрощение управления сетью

Сетевые возможности в ОС Windows Vista спроектированы с поддержкой управляемости по всем основным параметрам, позволяющей сократить расходы на внедрение беспроводных сетей и политик сетевой безопасности, а также обеспечить высокое качество обслуживания приложений и пользователей.

Для управления сетевыми функциями в ОС Windows Vista широко используются сценарии групповой политики или командной строки, выполняемые в сетевой оболочке NETSH, поэтому не требуется изучать или внедрять новый инструмент управления, а можно получить большую отдачу от вложенных средств в систему Active Directory и использовать созданную структуру подразделения.

Внедрение правил сетевой безопасности (с объединением политик сетевого экрана и службы IPsec) и управление этими правилами упрощается благодаря использованию одного встроенного в консоль управления MMC приложения (сетевого экрана с дополнительными функциями безопасности) с подсказками для пользователя или сценариев командной строки, выполняемых в оболочке NETSH.

Это новое встроенное приложение позволяет реализовать правила фильтрации входящих или исходящих потоков, а также правила установления безопасной связи, ограничивающие доступ конкретным пользователям, компьютерам или приложениям с обеспечением административного управления.

Для обеспечения соответствия политике безопасности на основе сценариев служба IPSec может затребовать проверку подлинности пользователей, компьютеров или отсутствия вирусов (совместно с функцией защиты сетевого доступа).

Встроенное приложение облегчает создание правил отделения сервера или домена, а поскольку оно работает на основе групповой политики, вы можете применять эти правила гибким образом, в зависимости от структуры вашей организации. При помощи групповой политики можно задавать способ подключения клиентов мобильных систем к беспроводным сетям и правила работы в этих сетях.

Например, в компании может быть принята политика, обязывающая использовать при всех беспроводных соединениях только один определенный протокол или устанавливать все соединения только с одной конкретной беспроводной сетью. Эти установки задаются при помощи групповой политики, что позволяет исключить вероятность изменения этих настроек конечным пользователем.

Windows Vista является самой мощной и безопасной из существующих на сегодняшний день операционных систем семейства Windows. Оптимизированная для решения бизнес-задач, Windows Vista обеспечивает значительные преимущества для предприятий:

- комплекс средств для защиты важной информации позволяет создать полностью безопасную ИТ-среду, соответствующую корпоративным стандартам безопасности;
- надежная защита данных обеспечена как при работе в сети предприятия, так и за ее пределами;
- мобильные пользователи и удаленные сотрудники могут легко подключаться к корпоративным ресурсам и работать с той же эффективностью, что и офисные пользователи.

Вопросы для самоконтроля

1. Сформулируйте понятие доверенной вычислительной базы.
2. Дайте определение защищенной операционной системы.
3. Опишите классификацию угроз безопасности операционной системы по различным аспектам их реализации.
4. Опишите типичные атаки, которым может подвергнуться операционная система.
5. Опишите основные функции подсистемы защиты операционной системы.
6. Определите основные понятия процесса разграничения доступа к объектам ОС.
7. Укажите основные особенности и различия избирательного и полномочного разграничения доступа.
8. Охарактеризуйте основные модели разграничения доступа, применяемые в ОС.
9. Каково назначение подсистемы аудита ОС и каким требованиям она должна удовлетворять?
10. Как осуществляется защита файловой системы ОС UNIX?
11. Охарактеризуйте безопасность системы UNIX при работе в сети.
12. Опишите основные функции и средства защиты, обеспечивающие безопасность операционной системы Windows Vista.

Глава 9
ПРОТОКОЛЫ ЗАЩИЩЕННЫХ КАНАЛОВ

Защита информации в процессе ее передачи по открытым каналам основана на построении виртуальных защищенных каналов связи, называемых криптозащищенными туннелями, или туннелями VPN. Каждый такой туннель представляет собой соединение, проведенное через открытую сеть, по которому передаются криптографически защищенные пакеты сообщений виртуальной сети.

Виртуальный защищенный канал можно построить с помощью системных средств, реализованных на разных уровнях модели взаимодействия открытых систем OSI. От выбранного рабочего уровня OSI зависит функциональность реализуемого виртуального защищенного канала и его совместимость с приложениями корпоративной информационной системы, а также с другими средствами защиты.

Для независимости от прикладных протоколов и приложений виртуальные защищенные каналы формируются на одном из более низких уровней модели OSI — канальном, сетевом или сеансовом.

Средства, применяемые на *канальном уровне* модели OSI, позволяют обеспечить инкапсуляцию различных видов трафика третьего уровня (и более высоких) и построение виртуальных туннелей типа точка—точка (от маршрутизатора к маршрутизатору или от персонального компьютера к шлюзу ЛВС).

Особенности защиты *на сетевом уровне* с помощью протоколов IPSec и IKE (Internet Key Exchange) разбираются в разделе 9.2.

При построении защищенных виртуальных каналов на *сеансовом уровне* появляется возможность криптографической защиты информационного обмена, включая аутентификацию, а также реализации ряда функций посредничества между взаимодействующими сторонами (см. раздел 9.3).

9.1. Защита на канальном уровне — протоколы PPTP, L2F и L2TP

Протоколы PPTP (Point-to-Point Tunneling Protocol), L2F (Layer-2 Forwarding) и L2TP (Layer-2 Tunneling Protocol) являются протоколами туннелирования канального уровня модели OSI. Общим свойством

этих протоколов является то, что они используются для организации защищенного многопротокольного удаленного доступа к ресурсам корпоративной сети через открытую сеть, например, через Интернет.

Все три протокола — PPTP, L2F и L2TP — обычно относят к протоколам формирования защищенного канала, однако этому определению точно соответствует только протокол PPTP, который обеспечивает туннелирование и шифрование передаваемых данных. Протоколы L2F и L2TP являются протоколами туннелирования, поскольку поддерживают только функции туннелирования. Функции защиты данных (шифрование, целостность, аутентификация) в этих протоколах не поддерживаются. Для защиты туннелируемых данных в этих протоколах необходимо использовать некоторый дополнительный протокол, в частности IPSec.

Клиентское программное обеспечение обычно использует для удаленного доступа стандартный протокол канального уровня PPP (Point-to-Point Protocol). Протоколы PPTP, L2F и L2TP основываются на протоколе PPP и являются его расширениями. Первоначально протокол PPP, расположенный на канальном уровне, был разработан для инкапсуляции данных и их доставки по соединениям типа точка—точка. Этот протокол служит также для организации асинхронных (например, коммутируемых) соединений.

В набор PPP входят протокол управления соединением LCP (Link Control Protocol), ответственный за конфигурацию, установку, работу и завершение соединения точка—точка, и протокол управления сетью NCP (Network Control Protocol), способный инкапсулировать в PPP протоколы сетевого уровня для транспортировки через соединение точка—точка. Это позволяет одновременно передавать пакеты Novell IPX и Microsoft IP по одному соединению PPP.

Для доставки конфиденциальных данных из одной точки в другую через сети общего пользования сначала производится инкапсуляция данных с помощью протокола PPP, затем протоколы PPTP и L2TP выполняют шифрование данных и собственную инкапсуляцию.

После того как туннельный протокол доставляет пакеты из начальной точки туннеля в конечную, выполняется деинкапсуляция.

На физическом и канальном уровнях протоколы PPTP и L2TP идентичны, но на этом их сходство заканчивается и начинаются различия.

9.1.1. Протокол PPTP

Протокол PPTP (Point-to-Point Tunneling Protocol), разработанный компанией «Майкрософт» при поддержке ряда других компаний, предназначен для создания защищенных виртуальных каналов при доступе удаленных пользователей к локальным сетям через Интернет. Протокол PPTP предполагает создание криптозащищенного туннеля на канальном уровне модели OSI для случаев как прямого соединения удаленного компьютера с открытой сетью, так и подсоединения его к открытой сети по телефонной линии через провайдера [7, 27].

Протокол PPTP получил практическое распространение благодаря компании «Майкрософт», реализовавшей его в своих операционных системах Windows NT/2000. Некоторые производители межсетевых экранов и шлюзов VPN также поддерживают протокол PPTP. Протокол PPTP позволяет создавать защищенные каналы для обмена данными по протоколам IP, IPX или NetBEUI. Данные этих протоколов упаковываются в кадры PPP и затем инкапсулируются посредством протокола PPTP в пакеты протокола IP, с помощью которого переносятся в зашифрованном виде через любую сеть TCP/IP.

Пакеты, передаваемые в рамках сессии PPTP, имеют следующую структуру (рис. 9.1):

- заголовок канального уровня, используемый внутри Интернета, например заголовок кадра Ethernet;
- заголовок IP, содержащий адреса отправителя и получателя пакета;
- заголовок общего метода инкапсуляции для маршрутизации GRE (Generic Routing Encapsulation);
- исходный пакет PPP, включающий пакет IP, IPX или NetBEUI.

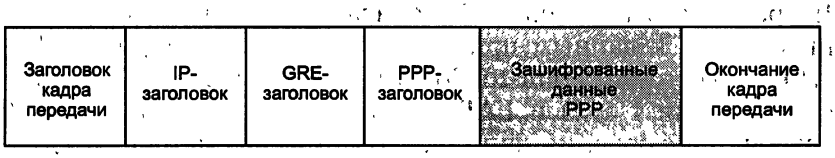


Рис. 9.1. Структура пакета для пересылки по туннелю PPTP

Принимающий узел сети извлекает из пакетов IP кадры PPP, а затем извлекает из кадра PPP исходный пакет IP, IPX или NetBEUI и отправляет его по локальной сети конкретному адресату. Многопротокольность инкапсулирующих протоколов канального уровня, к которым относится протокол PPTP, является их важным преимуществом перед протоколами защищенного канала более высоких уровней. Например, если в корпоративной сети используются IPX или NetBEUI, применение протоколов IPSec или SSL просто невозможно, поскольку они ориентированы только на один протокол сетевого уровня IP.

Данный способ инкапсуляции обеспечивает независимость от протоколов сетевого уровня модели OSI и позволяет осуществлять защищенный удаленный доступ через открытые IP-сети к любым локальным сетям (IP, IPX или NetBEUI). Согласно протоколу PPTP при создании защищенного виртуального канала производится аутентификация удаленного пользователя и шифрование передаваемых данных (рис. 9.2).

Для аутентификации удаленного пользователя могут использоваться различные протоколы, применяемые для PPP. В реализации PPTP, включенной компанией «Майкрософт» в Windows NT/2000, поддерживаются следующие протоколы аутентификации: протокол аутентификации по паролю PAP (Password Authentication Protocol), протокол аутентификации при рукопожатии MSCHAP (Microsoft Challenge-Handshaking Authentication Protocol) и протокол аутентификации EAP-TLS (Extensible

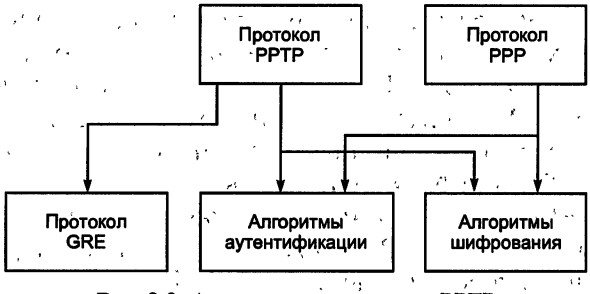


Рис. 9.2. Архитектура протокола PPTP

Authentication Protocol-Transport Layer Security). При использовании протокола PAP идентификаторы и пароли передаются по линии связи в незашифрованном виде, при этом только сервер проводит аутентификацию клиента. При использовании протоколов MSCHAP и EAP-TLS обеспечиваются защита от повторного использования злоумышленником перехваченных пакетов с зашифрованным паролем и взаимная аутентификация клиента и VPN-сервера.

Шифрование с помощью PPTP гарантирует, что никто не сможет получить доступ к данным при пересылке через Интернет. Шифрование MPPE (Microsoft Point-to-Point Encryption) совместимо только с MSCHAP (версии 1 и 2) и EAP-TLS и умеет автоматически выбирать длину ключа шифрования при согласовании параметров между клиентом и сервером. Шифрование MPPE поддерживает работу с ключами длиной 40, 56 или 128 бит. Протокол PPTP изменяет значение ключа шифрования после каждого принятого пакета.

Протокол PPTP применяется в схеме туннелирования при прямом подсоединении компьютера удаленного пользователя к Интернету [27, 41]. Рассмотрим реализацию этой схемы туннелирования (рис. 9.3). Удаленный пользователь устанавливает удаленное соединение с локальной сетью с помощью клиентской части сервиса удаленного доступа

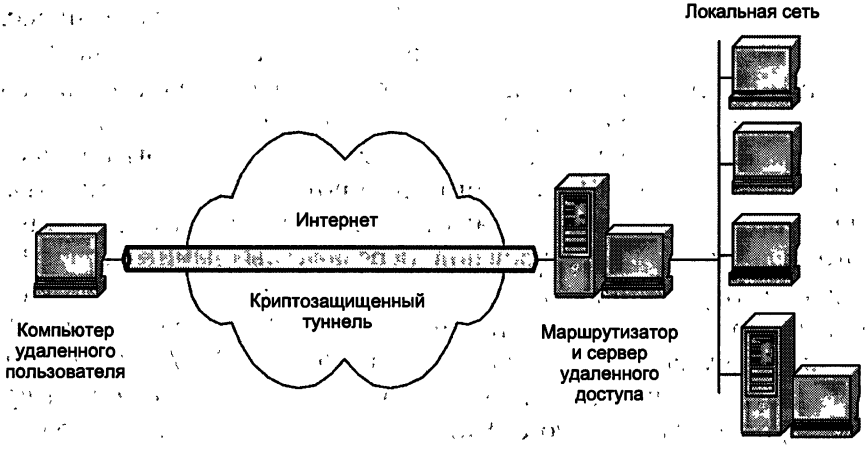


Рис. 9.3. Схема туннелирования при прямом подсоединении компьютера удаленного пользователя к Интернету

RAS (Remote Access Service), входящего в состав Windows. Затем пользователь обращается к серверу удаленного доступа локальной сети, указывая его IP-адрес, и устанавливает с ним связь по протоколу PPTP.

Функции сервера удаленного доступа может выполнять пограничный маршрутизатор локальной сети. На компьютере удаленного пользователя должны быть установлены клиентская часть сервиса RAS и драйвер PPTP, которые входят в состав Windows 98/NT, а на сервере удаленного доступа локальной сети — сервер RAS и драйвер PPTP, входящие в состав Windows NT Server. Протокол PPTP определяет несколько служебных сообщений, которыми обмениваются взаимодействующие стороны. Служебные сообщения передаются по протоколу TCP.

После успешной аутентификации начинается процесс защищенного информационного обмена. Внутренние серверы локальной сети могут не поддерживать протокол PPTP, поскольку пограничный маршрутизатор извлекает кадры PPP из пакетов IP и посылает их по локальной сети в необходимом формате — IP, IPX или NetBIOS.

9.1.2. Протоколы L2F и L2TP

Протокол L2F (Layer-2 Forwarding) был разработан компанией Cisco Systems для построения защищенных виртуальных сетей на канальном уровне модели OSI как альтернатива протоколу PPTP. По сравнению с PPTP протокол L2F отличается поддержкой разных сетевых протоколов и более удобен в использовании для провайдеров Интернета. Для организации связи компьютера удаленного пользователя с сервером провайдера протокол L2F допускает применение различных протоколов удаленного доступа PPP, SLIP и др. Открытая сеть, используемая для переноса пакетов через туннель, может функционировать на основе как протокола IP, так и других протоколов, в частности X.25.

Недостатки протокола L2F:

- в протоколе L2F не предусмотрено создание для текущей версии протокола IP криптозащищенного туннеля между конечными точками информационного взаимодействия;
- виртуальный защищенный канал может быть создан только между сервером удаленного доступа провайдера и пограничным маршрутизатором локальной сети, при этом участок между компьютером удаленного пользователя и сервером провайдера остается открытым.

Протокол L2F был фактически поглощен протоколом L2TP, имеющим статус проекта стандарта Интернета, поэтому далее будут рассматриваться основные возможности и свойства протокола L2TP.

Протокол L2TP (Layer-2 Tunneling Protocol) разработан в организации IETF (Internet Engineering Task Force) при поддержке компаний «Майкрософт» и Cisco Systems. Протокол L2TP разрабатывался как протокол защищенного туннелирования PPP-трафика через сети общего назначения с произвольной средой. Работа над этим протоколом ве-

лась на основе протоколов PPTP и L2F, и в результате он вобрал в себя лучшие качества исходных протоколов [7].

В отличие от PPTP, протокол L2TP не привязан к протоколу IP, поэтому он может быть использован в сетях с коммутацией пакетов, например в сетях ATM (Asynchronous Transfer Mode) или в сетях с ретрансляцией кадров (Frame Relay). Кроме того, в протокол L2TP добавлена отсутствующая в протоколе L2F важная функция управления потоками данных.

В протоколе L2TP не только объединены лучшие свойства протоколов PPTP и L2F, но и добавлены новые функции. В протокол L2TP добавлен ряд отсутствующих в спецификации протокола PPTP функций защиты, в частности, включена возможность работы с протоколами AH и ESP стека протоколов IPSec. Архитектура протокола L2TP представлена на рис. 9.4.

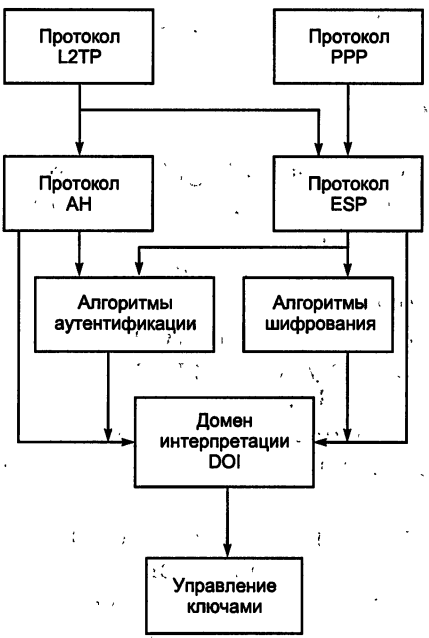


Рис. 9.4. Архитектура протокола L2TP

Протоколы AH и ESP являются основными компонентами стека протоколов IPSec. Эти протоколы допускают использование пользователями по их согласованному выбору различных криптографических алгоритмов шифрования и аутентификации. На домен интерпретации DOI (Domain of Interpretation) возложены функции обеспечения совместной работы используемых протоколов и алгоритмов. Применение стека протоколов IPSec для организации защищенных каналов подробно рассматривается в разделе 9.2.

В сущности, гибридный протокол L2TP представляет собой расширение протокола PPP функциями аутентификации удаленных пользова-

телей, создания защищенного виртуального соединения и управления потоками данных.

Протокол L2TP применяет в качестве транспорта протокол UDP и использует одинаковый формат сообщений как для управления туннелем, так и для пересылки данных. В реализации «Майкрософт» протокол L2TP использует в качестве контрольных сообщений пакеты UDP, содержащие шифрованные пакеты PPP. Надежность доставки гарантирует контроль последовательности пакетов.

Как и в случае с PPTP, протокол L2TP начинает сборку пакета для передачи в туннель с того, что к полю информационных данных PPP добавляется сначала заголовок PPP, а затем заголовок L2TP. Полученный таким образом пакет инкапсулируется протоколом UDP. В качестве порта отправителя и получателя протокол L2TP использует UDP-порт 1701. На рис. 9.5 показана структура пакета для пересылки по туннелю L2TP.

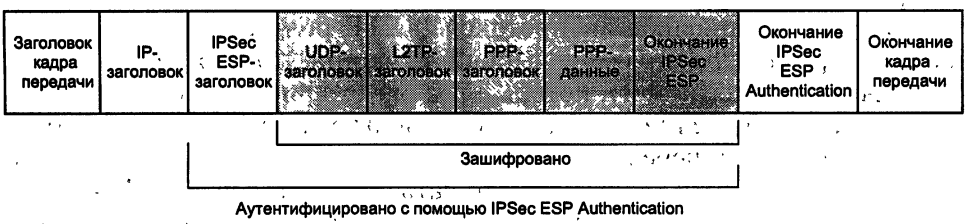


Рис. 9.5. Структура пакета для пересылки по туннелю L2TP

В зависимости от выбранного типа политики безопасности стека протоколов IPSec, протокол L2TP может шифровать UDP-сообщения и добавлять к ним заголовок и окончание ESP (Encapsulating Security Payload), а также окончание IPSec ESP Authentication. Затем производится инкапсуляция в IP. Добавляется IP-заголовок, содержащий адреса отправителя и получателя. В завершение L2TP выполняет вторую PPP-инкапсуляцию для подготовки данных к передаче.

Компьютер-получатель принимает данные, обрабатывает заголовок и окончание PPP, убирает заголовок IP. При помощи IPSec ESP Authentication проводится аутентификация информационного поля IP, а протокол ESP IPSec помогает расшифровать пакет. Далее компьютер обрабатывает заголовок UDP и использует заголовок L2TP для идентификации туннеля. Теперь пакет PPP содержит только полезные данные, которые обрабатываются или пересылаются указанному получателю.

Хотя протокол PPTP обеспечивает достаточную степень безопасности, но все же протокол L2TP (поверх IPSec) надежнее. Протокол L2TP поверх IPSec обеспечивает аутентификацию на уровнях «пользователь» и «компьютер», а также выполняет аутентификацию и шифрование данных. На первом этапе аутентификации клиентов и серверов VPN протокол L2TP использует локальные сертификаты, полученные от службы сертификации. Клиент и сервер обмениваются сертификатами и создают защищенное соединение ESP SA (Security Association).

После того как L2TP (поверх IPSec) завершает процесс аутентификации компьютера, выполняется аутентификация на уровне пользователя. Для этой аутентификации можно задействовать любой протокол, даже PAP, передающий имя пользователя и пароль в открытом виде. Это вполне безопасно, так как L2TP (поверх IPSec) шифрует всю сессию. Однако проведение аутентификации пользователя при помощи MSCHAP, применяющего различные ключи шифрования для аутентификации компьютера и пользователя, может повысить безопасность.

Протокол L2TP предполагает использование схемы, в которой туннель образуется между сервером удаленного доступа провайдера и маршрутизатором корпоративной сети. В отличие от своих предшественников — протоколов PPTP и L2F, — протокол L2TP предоставляет возможность открывать между конечными абонентами сразу несколько туннелей, каждый из которых может быть выделен для отдельного приложения. Эти особенности обеспечивают гибкость и безопасность туннелирования.

Согласно спецификации протокола L2TP роль сервера удаленного доступа провайдера должен выполнять концентратор доступа LAC (L2TP Access Concentrator), который реализует клиентскую часть протокола L2TP и обеспечивает удаленному пользователю сетевой доступ к его локальной сети через Интернет. В качестве сервера удаленного доступа локальной сети должен выступать сетевой сервер LNS (L2TP Network Server), функционирующий на совместимых с протоколом PPP платформах (рис. 9.6).

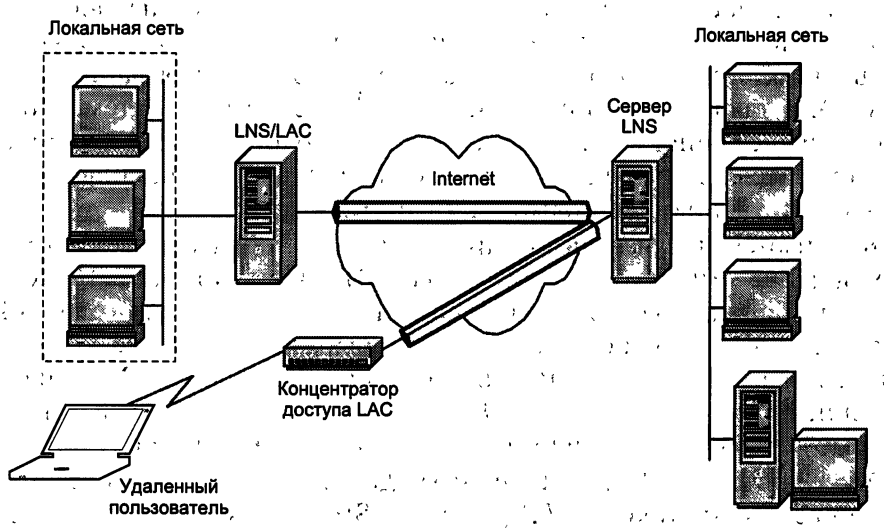


Рис. 9.6. Схемы туннелирования по протоколу L2TP

Аналогично протоколам PPTP и L2F формирование защищенного виртуального канала в протоколе L2TP осуществляется в три этапа:

- установление соединения с сервером удаленного доступа локальной сети;

- аутентификация пользователя;
- конфигурирование защищенного туннеля [7].

На первом этапе для установления соединения с сервером удаленного доступа локальной сети удаленный пользователь инициирует PPP-соединение с провайдером ISP. Концентратор доступа LAC, функционирующий на сервере провайдера ISP, принимает это соединение и устанавливает канал PPP. Затем концентратор доступа LAC выполняет частичную аутентификацию конечного узла и его пользователя. Используя только имя пользователя, провайдер ISP решает, нужен ли пользователю сервис туннелирования L2TP. Если такой сервис нужен, то следующим шагом для концентратора доступа LAC будет выяснение адреса сетевого сервера LNS, с которым нужно установить туннельное соединение. Для удобства определения соответствия между пользователем и сервером LNS, обслуживающим сеть пользователя, может использоваться база данных, поддерживаемая провайдером ISP для своих клиентов.

После выяснения IP-адреса сервера LNS производится проверка, не существует ли уже туннель L2TP с этим сервером. Если такого туннеля нет, то он устанавливается. Между концентратором доступа провайдера LAC и сетевым сервером LNS локальной сети устанавливается сессия по протоколу L2TP.

Протокол L2TP разработан с максимальным абстрагированием от деталей транспорта открытой сети, через которую прокладывается туннель. Основное требование, которое предъявляется к транспорту, заключается в том, чтобы он поддерживал пакетный режим взаимодействия точка—точка. В качестве такого транспорта может быть использован протокол UDP, коммутируемые виртуальные соединения X.25 или постоянные виртуальные соединения Frame Relay. При создании туннеля между LAC и LNS новому соединению в рамках этого туннеля присваивается идентификатор, называемый идентификатором вызова Call ID. Концентратор LAC отправляет сетевому серверу LNS пакет с уведомлением о вызове с данным Call ID. Сервер LNS может принять этот вызов или отклонить его.

На втором этапе после установления сессии L2TP сетевой сервер LNS локальной сети выполняет процесс аутентификации пользователя. Для этого может быть использован один из стандартных алгоритмов аутентификации, в частности CHAP. Следует отметить, что в спецификации протокола L2TP не приводятся описания методов аутентификации. Уведомление о вызове может включать информацию для аутентификации пользователя сетевым сервером LNS. Эту информацию собирает концентратор LAC в процессе общения с пользователем. В случае применения протокола аутентификации CHAP пакет уведомления включает слово-вызов, имя пользователя и его ответ. Для протокола PAP эта информация состоит из имени пользователя и незашифрованного пароля. Сетевой сервер LNS может сразу использовать эту информацию для выполнения аутентификации, чтобы не заставлять удаленного пользователя повторно вводить свои данные и не осуществлять дополнительный цикл аутентификации.

При отправке результата аутентификации сетевой сервер LNS может также передать концентратору доступа LAC сведения об IP-адресе узла пользователя. По существу, коцентратор доступа LAC работает как посредник между узлом удаленного пользователя и сетевым сервером LNS локальной сети. Выделение адреса для удаленного узла из пула адресов корпоративной сети позволяет избежать неудобств, с которыми сталкивается удаленный пользователь при обычном получении адреса из пула адресов провайдера.

На третьем этапе в случае успешной аутентификации пользователя создается защищенный туннель между концентратором доступа LAC провайдера и сервером LNS локальной сети. В результате инкапсулированные кадры PPP могут передаваться по туннелю между концентратором LAC и сетевым сервером LNS в обоих направлениях. При поступлении кадра PPP от удаленного пользователя концентратор LAC удаляет из него байты обрамления кадра, байты контрольной суммы, затем инкапсулирует его с помощью протокола L2TP в сетевой протокол и отправляет по туннелю сетевому серверу LNS. Сервер LNS, используя протокол L2TP, извлекает из прибывшего пакета кадр PPP и обрабатывает его стандартным образом.

Настройка необходимых значений параметров туннеля производится с помощью управляющих сообщений. Протокол L2TP может работать поверх любого транспорта с коммуникацией пакетов. В общем случае этот транспорт, например протокол UDP, не обеспечивает гарантированной доставки пакетов. Поэтому протокол L2TP самостоятельно решает эти вопросы, используя процедуры установления соединения внутри туннеля для каждого удаленного пользователя.

Следует отметить, что протокол L2TP не определяет конкретных методов криптозащиты и предполагает возможность применения различных стандартов шифрования. Если защищенный туннель планируется сформировать в IP-сетях, тогда для реализации криптозащиты используется протокол IPSec. Протокол L2TP поверх IPSec обеспечивает более высокую степень защиты данных, чем PPTP, так как использует алгоритмы шифрования 3-DES (Triple Data Encryption Standard) и AES. Кроме того, при помощи алгоритма HMAC (Hash Message Authentication Code) протокол L2TP обеспечивает аутентификацию данных. Для аутентификации данных этот алгоритм создает хэш длиной 128 разрядов.

Таким образом, функциональные возможности протоколов PPTP и L2TP различны. Протокол PPTP может применяться только в IP-сетях, и ему необходимо отдельное соединение TCP для создания и использования туннеля. Протокол L2TP может использоваться не только в IP-сетях, служебные сообщения для создания туннеля и пересылки по нему данных используют одинаковый формат и протоколы. Протокол L2TP поверх IPSec предлагает больше уровней безопасности, чем PPTP, и может гарантировать почти 100-процентную безопасность важных для организации данных.

Положительные качества протокола L2TP делают его весьма перспективным для построения виртуальных защищенных сетей. Однако

при всех своих достоинствах протокол L2TP не способен преодолеть ряд недостатков туннельной передачи данных на канальном уровне:

- для реализации протокола L2TP необходима поддержка провайдеров ISP;
- протокол L2TP ограничивает трафик рамками выбранного туннеля и лишает пользователей доступа к другим частям Интернета;
- в протоколе L2TP не предусмотрено создание для текущей версии протокола IP криптозащищенного туннеля между конечными точками информационного взаимодействия;
- предложенная спецификация L2TP обеспечивает стандартное шифрование только в IP-сетях с помощью протокола IPSec.

9.2. Защита на сетевом уровне — протокол IPSec

Радикальное устранение уязвимостей компьютерных сетей возможно при создании системы защиты не для отдельных классов приложений, а для сети в целом. Применительно к IP-сетям это означает, что системы защиты должны действовать на сетевом уровне модели OSI. Преимущество такого выбора заключается в том очевидном факте, что в IP-сетях именно сетевой уровень отличается наибольшей гомогенностью: независимо от вышележащих протоколов, физической среды передачи и технологии канального уровня транспортировка данных по сети не может быть произведена в обход протокола IP. Поэтому реализация защиты сети на третьем уровне автоматически гарантирует как минимум такую же степень защиты всех сетевых приложений, причем без какой-либо модификации последних.

При формировании защищенных виртуальных каналов на сетевом уровне модели OSI достигается оптимальное соотношение между прозрачностью и качеством защиты. Размещение средств защиты на сетевом уровне делает их прозрачными для приложений, так как между сетевым уровнем и приложением функционирует реализация протокола транспортного уровня. Для пользователей процедуры защиты оказываются столь же прозрачными, как и сам протокол IP. На сетевом уровне существует возможность достаточно полной реализации функций защиты трафика и управления ключами, поскольку именно на сетевом уровне выполняется маршрутизация пакетов сообщений.

Стек протоколов IPSec (Internet Protocol Security) используется для аутентификации участников обмена, туннелирования трафика и шифрования IP-пакетов. Основное назначение протокола IPSec — обеспечение безопасной передачи данных по сетям IP. Поскольку архитектура IPSec обеспечивает его совместимость с протоколом IPv4, ее поддержку достаточно обеспечить на обоих концах соединения; промежуточные сетевые узлы могут вообще ничего «не знать» об IPSec. Протокол IPSec может защищать трафик как текущей версии протокола IPv4, применяемой сегодня в Интернете, так и новой версии IPv6, которая постепенно внедряется в Интернет.

9.2.1. Архитектура средств безопасности IPSec

Основное назначение протоколов IPSec — обеспечение безопасной передачи данных по сетям IP. Применение IPSec гарантирует:

- целостность передаваемых данных, т. е. данные при передаче не искажены, не потеряны и не продублированы;
- аутентичность отправителя, т. е. данные переданы именно тем отправителем, который доказал, что он тот, за кого себя выдает;
- конфиденциальность передаваемых данных, т. е. данные передаются в форме, предотвращающей их несанкционированный просмотр.

Следует отметить, что обычно в понятие безопасности данных включают еще одно требование — доступность данных, что в рассматриваемом контексте можно интерпретировать как гарантию их доставки. Протоколы IPSec не решают данную задачу, оставляя ее протоколу транспортного уровня TCP. Стек протоколов IPSec обеспечивает защиту информации на сетевом уровне, что делает эту защиту невидимой для работающих приложений.

Фундаментальной единицей коммуникации в IP-сетях является IP-пакет. Структура IP-пакета показана на рис. 9.7. IP-пакет содержит S-адрес источника и D-адрес получателя сообщения, транспортный заголовок, информацию о типе данных, переносимых в этом пакете, и сами данные.

Рис. 9.7. Структура IP-пакета

Пользователь воспринимает сеть как надежно защищенную среду только в том случае, если он уверен, что его партнер по обмену — именно тот, за кого он себя выдает (аутентификация сторон), что передаваемые пакеты не просматриваются посторонними лицами (конфиденциальность связи) и что получаемые данные не подверглись изменению в процессе передачи (целостность данных).

Для того чтобы обеспечить аутентификацию, конфиденциальность и целостность передаваемых данных, стек протоколов IPSec построен на базе ряда стандартизованных криптографических технологий:

- обмены ключами согласно алгоритму Диффи — Хеллмана для распределения секретных ключей между пользователями в открытой сети;
- криптография открытых ключей для подписывания обменов Диффи — Хеллмана, чтобы гарантировать подлинность двух сторон и избежать атак типа «человек-в-середине»;
- цифровые сертификаты для подтверждения подлинности открытых ключей;
- блочные симметричные алгоритмы шифрования данных;

- алгоритмы аутентификации сообщений на базе функций хэширования.

Протокол IPSec определяет стандартные способы защиты информационного обмена на сетевом уровне модели OSI для IP-сети, являющейся основным видом окрытых сетей. Данный протокол входит в состав новой версии протокола IP (IPv6) и применим также к его текущей версии (IPv4). Для протокола IPv4 поддержка IPSec является желательной, а для IPv6 — обязательной. Протокол IPSec представляет собой систему открытых стандартов, которая имеет четко очерченное ядро и которую можно дополнять новыми протоколами, алгоритмами и функциями. Стандартизованными функциями IPSec-защиты могут пользоваться протоколы более высоких уровней, в частности управляющие протоколы, протоколы конфигурирования, а также протоколы маршрутизации.

Основными задачами установления и поддержания защищенного канала являются следующие:

- аутентификация пользователей или компьютеров при инициации защищенного канала;
- шифрование и аутентификация передаваемых данных между конечными точками защищенного канала;
- обеспечение конечных точек канала секретными ключами, необходимыми для работы протоколов аутентификации и шифрования данных.

Для решения перечисленных задач система IPSec использует комплекс средств безопасности информационного обмена.

Большинство реализаций протокола IPSec имеют следующие компоненты:

- основной протокол IPSec. Этот компонент реализует ESP и AH. Он обрабатывает заголовки, взаимодействует с базами данных SPD и SAD для определения политики безопасности, применяемой к пакету;
- протокол управления обменом ключевой информации IKE (Internet Key Exchange). IKE обычно представляется как процесс пользовательского уровня, за исключением реализаций, встроенных в операционную систему;
- базу данных политик безопасности SPD (Security Policy Database). Это один из важнейших компонентов, поскольку он определяет политику безопасности, применяемую к пакету. SPD используется основным протоколом IPSec при обработке входящих и исходящих пакетов;
- базу данных безопасных ассоциаций SAD (Security Association Database). База данных SAD хранит список безопасных ассоциаций SA (Security Association) для обработки входящей и исходящей информации. Исходящие SA используются для защиты исходящих пакетов, а входящие SA — для обработки пакетов с заголовками IPSec. База данных SAD заполняется SA вручную или с помощью протокола управления ключами IKE;

- управление политикой безопасности и безопасными ассоциациями SA. Это приложения, которые управляют политикой безопасности и SA [7].

Основной протокол IPSec (реализующий ESP и AH) тесно взаимодействует с транспортным и сетевым уровнями стека протоколов TCP/IP. Фактически протокол IPSec является частью сетевого уровня. Основной модуль протокола IPSec обеспечивает два интерфейса: входной и выходной. Входной интерфейс используется входящими пакетами, а выходной — исходящими. Реализация IPSec не должна зависеть от интерфейса между транспортным и сетевым уровнями стека протоколов TCP/IP.

Базы данных SPD и SAD существенно влияют на эффективность работы IPSec. Выбор структуры данных для хранения SPD и SAD является критическим моментом, от которого зависит производительность IPSec. Особенности реализации SPD и SAD зависят от требований производительности и совместимости системы.

Все протоколы, входящие в IPSec, можно разделить на две группы:

- протоколы, непосредственно производящие обработку передаваемых данных (для обеспечения их защиты);
- протоколы, позволяющие автоматически согласовать параметры защищенных соединений, необходимые для протоколов первой группы.

Ядро IPSec составляют три протокола: протокол аутентифицирующего заголовка AH (Authentication Header), протокол инкапсулирующей защиты ESP (Encapsulating Security Payload) и протокол согласования параметров виртуального канала и управления ключами IKE (Internet Key Exchange).

Архитектура средств безопасности IPSec представлена на рис. 9.8.

На *верхнем уровне* расположены следующие протоколы:

- протокол согласования параметров виртуального канала и управления ключами IKE, определяющий способ инициализации за-

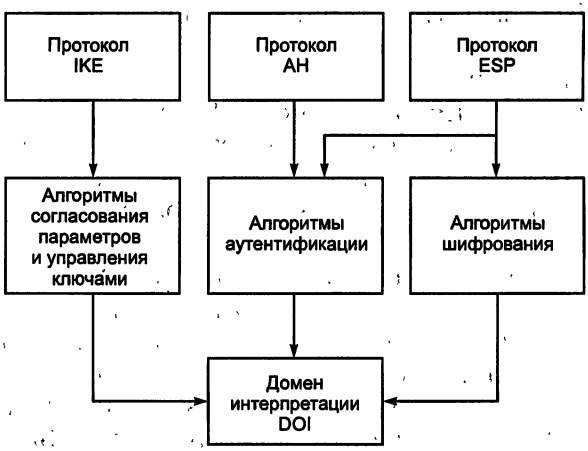


Рис. 9.8. Архитектура стека протоколов IPSec

щищенного канала, включая согласование используемых алгоритмов криптозащиты, а также процедуры обмена и управления секретными ключами в рамках защищенного соединения;

- протокол аутентифицирующего заголовка AH, обеспечивающий аутентификацию источника данных, проверку их целостности и подлинности после приема, а также защиту от навязывания повторных сообщений;
- протокол инкапсулирующей защиты содержимого ESP, обеспечивающий криптографическое закрытие, аутентификацию и целостность передаваемых данных, а также защиту от навязывания повторных сообщений.

Разделение функций защиты между двумя протоколами AH и ESP обусловлено применяемой во многих странах практикой ограничения экспорта и/или импорта средств, обеспечивающих конфиденциальность данных путем шифрования. Каждый из протоколов AH и ESP может использоваться как самостоятельно, так и совместно с другим. Из краткого перечисления функций протоколов AH и ESP видно, что возможности этих протоколов частично перекрываются.

Протокол AH отвечает только за обеспечение целостности и аутентификации данных, в то время как протокол ESP является более мощным, поскольку может шифровать данные, а кроме того, способен выполнять функции протокола AH (хотя, как увидим позднее, аутентификация и целостность обеспечиваются им в несколько урезанном виде).

Протокол ESP может поддерживать функции шифрования и аутентификации/обеспечения целостности в любых комбинациях, т. е. либо и ту и другую группу функций, либо только аутентификацию/обеспечение целостности, либо только шифрование.

Для шифрования данных в IPSec (протокол ESP) может быть применен практически любой симметричный алгоритм шифрования с секретными ключами. Для обеспечения целостности и аутентификации данных (протоколы AH и ESP) используется один из приемов шифрования — *шифрование с помощью односторонней функции* (One-way Function), называемой также дайджест-функцией (Digest Function) [7].

Протоколы IKE, AH и ESP взаимодействуют следующим образом.

Сначала с помощью протокола IKE между двумя точками устанавливается логическое соединение, которое в стандартах IPSec получило название «безопасная ассоциация» SA. При установлении этого логического соединения выполняется аутентификация конечных точек канала, а также выбираются параметры защиты данных, например алгоритм шифрования, сессионный секретный ключ и т. п.

Затем в рамках установленной безопасной ассоциации SA начинает работать протокол AH или ESP, с помощью которого и выполняется требуемая защита передаваемых данных с использованием выбранных параметров.

Средний уровень архитектуры IPSec образуют алгоритмы согласования параметров и управления ключами, применяемые в протоколе IKE, а также алгоритмы аутентификации и шифрования, используемые в

протоколах аутентифицирующего заголовка AH и инкапсулирующей защиты содержимого ESP.

Следует отметить, что протоколы защиты виртуального канала верхнего уровня архитектуры IPSec (AH и ESP) не зависят от конкретных криптографических алгоритмов. За счет возможности использования большого количества разнообразных алгоритмов аутентификации и шифрования IPSec обеспечивает высокую степень гибкости организации защиты сети. Гибкость IPSec состоит в том, что для каждой задачи предлагается несколько способов ее решения. Выбранные методы для одной задачи обычно не зависят от методов реализации других задач. Например, выбор для шифрования алгоритма DES не влияет на выбор функции вычисления дайджеста, используемого для аутентификации данных.

Нижний уровень архитектуры IPSec образует так называемый домен интерпретации DOI. Необходимость применения домена интерпретации DOI обусловлена следующими причинами. Протоколы AH и ESP имеют модульную структуру, допуская применение пользователями по их согласованному выбору различных криптографических алгоритмов шифрования и аутентификации. Поэтому необходим модуль, который мог бы обеспечить совместную работу всех применяемых и вновь включаемых протоколов и алгоритмов. Именно такие функции возложены на домен интерпретации DOI. Домен интерпретации DOI в качестве базы данных хранит сведения об используемых в IPSec протоколах и алгоритмах, их параметрах, протокольных идентификаторах и т. п. По существу, домен интерпретации DOI выполняет роль фундамента в архитектуре IPSec. Для того чтобы использовать алгоритмы, соответствующие национальным стандартам в качестве алгоритмов аутентификации и шифрования в протоколах AH и ESP, необходимо зарегистрировать эти алгоритмы в домене интерпретации DOI [7].

Для того чтобы протоколы AH и ESP могли выполнять свою работу по защите передаваемых данных, между конечными узлами необходимо установить безопасную ассоциацию SA. Цель SA — обеспечить достоверную идентификацию каждого конечного узла (данный процесс называется взаимной аутентификацией конечных узлов) и установить согласованные параметры защищенного соединения. Для установления безопасной ассоциации SA между двумя конечными точками используется протокол ISAKMP (Internet Security Association and Key Management Protocol), входящий в состав протокола согласования параметров виртуального канала и управления ключами IKE.

Установление SA начинается со взаимной аутентификации сторон. Выбираемые далее параметры SA определяют, какой из двух протоколов, AH или ESP, применяется для защиты данных, какие функции выполняет протокол защиты: например, только аутентификацию и проверку целостности или, кроме того, и защиту конфиденциальности данных. Важным параметром безопасной ассоциации SA является так называемый ключевой материал, т. е. секретные криптографические ключи, используемые в работе протоколов AH и ESP. В целях безопас-

ности IPSec никогда не пересылает ключи по сети; пересылаются данные, необходимые каждому конечному узлу, чтобы локально генерировать ключ.

Параметры безопасной ассоциации должны устраивать обе конечные точки защищенного канала. Поэтому при использовании автоматической процедуры установления SA протоколы IKE, работающие по разные стороны канала, выбирают параметры на основе взаимного согласования. Для каждой задачи, решаемой протоколами AH и ESP, предлагается несколько схем аутентификации и шифрования. Все это делает IPSec очень гибким средством защиты передаваемых данных.

Безопасная ассоциация SA представляет собой в IPSec однонаправленное логическое соединение, поэтому при двустороннем обмене данными необходимо установить две ассоциации SA. После того как между конечными узлами согласованы параметры шифрования, хэш-алгоритм и методы аутентификации, эти узлы создают одно соединение SA для входящих пакетов данных и другое — для исходящих.

Протоколы AH или ESP функционируют уже в рамках установленного логического соединения SA, с его помощью и осуществляется требуемая защита передаваемых данных с использованием выбранных параметров.

9.2.2. Защита передаваемых данных с помощью протоколов AH и ESP

Протокол аутентифицирующего заголовка AH и протокол инкапсулирующей защиты содержимого ESP могут работать в туннельном или транспортном режимах. Для выполнения своих задач по обеспечению безопасной передачи данных протоколы AH и ESP включают в обрабатываемые ими пакеты дополнительную служебную информацию, оформляя ее в виде заголовков. Ниже мы рассмотрим подробнее содержимое заголовков AH и ESP и связанную с ними функциональность.

Протокол аутентифицирующего заголовка AH

Протокол аутентифицирующего заголовка AH обеспечивает проверку аутентичности и целостности IP-пакетов, а также защиту от воспроизведения ранее посланных IP-пакетов.

Протокол AH позволяет приемной стороне убедиться в следующем:

- пакет был отправлен именно той стороной, с которой установлена данная ассоциация;
- содержимое пакета не подверглось искажениям в процессе передачи его по сети;
- пакет не является дубликатом некоторого пакета, полученного ранее.

Протокол AH полностью защищает от подлога и искажения содержимого IP-пакетов, включая данные протоколов более высоких уров-

ней. Полнота защиты полей IP-заголовков зависит от используемого режима работы — туннельного или транспортного.

Однако протокол AH не обеспечивает конфиденциальность передаваемых данных, т. е. он не предназначен для их шифрования. Данные могут быть прочитаны промежуточными узлами, но не могут быть изменены. Целостность и аутентичность данных обеспечиваются добавлением аутентифицирующего заголовка (AH) перед заголовком IP и заголовком транспортного уровня (TCP/UDP). Формат заголовка AH показан на рис. 9.9.

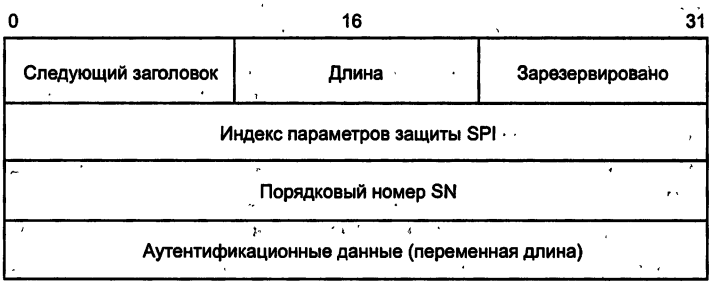


Рис. 9.9. Формат заголовка AH

Заголовок AH включает в себя следующие поля:

- *следующий заголовок (Next Header)* — однобайтовое поле, содержащее код протокола следующего заголовка, вложенного в IPSec-пакет, например код протокола TCP или ESP, чей заголовок следует за AH;
- *длина (Payload Len)* — указывает длину заголовка AH в 32-битных словах;
- *индекс параметров защиты SPI (Security Parameters Index)* — представляет собой 32-разрядную метку безопасной ассоциации SA, содержащей все параметры туннеля IPSec, включая типы криптографических алгоритмов и ключи шифрования. На основании индекса SPI пакет будет правильно отнесен к одной из существующих ассоциаций в приемном шлюзе (или хосте). Если же активной ассоциации, на которую указывает метка SPI, не существует, то пакет просто отбрасывается;
- *порядковый номер SN (Sequence Number)* — беззнаковое 32-битное число, увеличиваемое на единицу после передачи каждого защищенного по протоколу AH IP-пакета. Обеспечивает защиту от ложного воспроизведения ранее посланных IP-пакетов. При формировании каждого защищенного сеанса информационного обмена в рамках туннеля IPSec взаимодействующие стороны делают свои счетчики нулевыми, а потом согласованным образом увеличивают их. Получатель проверяет это поле с целью удостовериться, что пакета с таким номером принято еще не было. Если же такой пакет уже был, он не принимается;
- *аутентификационные данные (Authentication Data)* — поле переменной длины, содержащее информацию, используемую для аутенти-

фикации пакета и называемую MAC-кодом (Message Authentication Code). Это поле называют также цифровой подписью, дайджестом или кодом проверки целостности ICV (Integrity Check Value) пакета. Содержимое поля Authentication Data вычисляется с помощью одного из двух обязательно поддерживаемых протоколом AH алгоритмов, HMAC-MD5 и HMAC-SHA1, основанных на применении односторонних хэш-функций с секретными ключами. Длина дайджеста зависит от выбранного алгоритма, так что это поле имеет в общем случае переменный размер. Наиболее часто используемый алгоритм HMAC-MD5 порождает 16-байтный дайджест.

Протокол AH защищает весь IP-пакет, за исключением некоторых полей в IP-заголовке, таких как время жизни (TTL) и тип службы (Type of Service), которые могут меняться в процессе передачи пакета в сети. Заметим, что протокол AH обеспечивает защиту от изменений IP-адресов в заголовке пакета. Протокол аутентификации AH создает своеобразный конверт, обеспечивающий аутентификацию источника данных, их целостность и защиту от навязывания повторных сообщений.

Протокол AH может быть использован в двух режимах:

- туннельном;
- транспортном.

Местоположение заголовка AH в пакете зависит от того, в каком режиме — транспортном или туннельном — сконфигурирован защищенный канал. На рис. 9.10 показано расположение AH-заголовка относительно IP-заголовка в обоих режимах.

В *транспортном режиме* заголовок исходного IP-пакета становится внешним заголовком, за ним следует заголовок AH, а затем — все данные защищаемого пакета (т. е. пакет протокола верхнего уровня). Протокол AH защищает весь полученный таким образом пакет, включая заголовок IP и собственно сам заголовок AH. Таким образом, любое изменение данных в пакете или заголовков будет обнаружено. Следует также заметить, что в этом режиме данные пакета отсылаются открытыми, т. е. мы защищаем данные пакета от изменений, но не можем за-

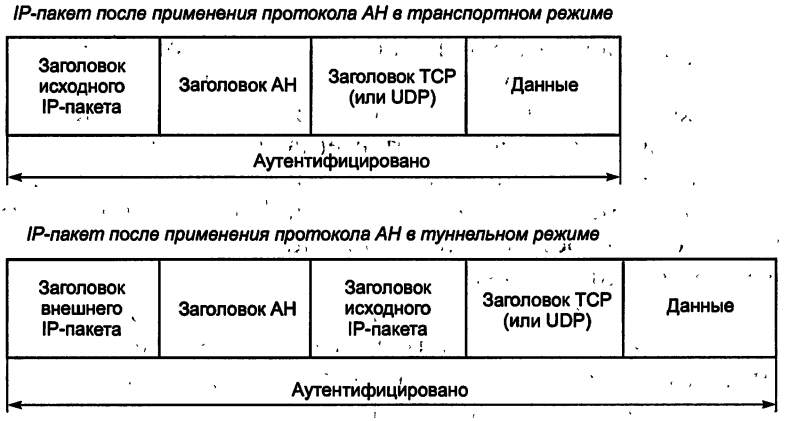


Рис. 9.10. IP-пакет после применения протокола AH в транспортном и туннельном режимах

щитить их от просмотра. В частности, не удается скрыть IP-адреса источника и назначения от возможного просмотра посторонними лицами, поскольку эти поля всегда присутствуют в незашифрованном виде и соответствуют действительным адресам хостов.

В *туннельном режиме* в качестве заголовка внешнего IP-пакета создается новый заголовок IP. IP-адреса посылающей и принимающей сторон могут отличаться от адресов в заголовке исходного IP-пакета. В защищенном IP-пакете внутренний (первоначальный) IP-заголовок содержит целевой адрес пакета, а внешний IP-заголовок — адрес конца туннеля. За новым заголовком внешнего IP-пакета следует заголовок AH, а затем весь исходный пакет (заголовок IP и сами данные). Как и в случае транспортного режима, протокол AH защищает весь созданный пакет (два заголовка IP, заголовок AH и данные), что также позволяет обнаружить любые изменения в пакете. Как и в транспортном режиме, сам пакет не защищен от просмотра.

Независимо от режима работы, протокол AH предоставляет меры защиты от атак, направленных на нарушение целостности и подлинности пакетов сообщений. С помощью этого протокола аутентифицируется каждый пакет, что делает программы, пытающиеся перехватить управление сеансом, неэффективными. Протокол AH обеспечивает аутентификацию не только содержимого, но и заголовков IP-пакетов. Однако следует иметь в виду, что аутентификация по протоколу AH не допускает манипулирование основными полями IP-заголовка во время прохождения пакета. По этой причине данный протокол нельзя применять в среде, где используется механизм трансляции сетевых адресов NAT (Network Address Translation), поскольку для его работы необходимо манипулирование IP-заголовками.

Протокол AH может применяться в одиночку и в комбинации с протоколом ESP или даже с пакетом, который уже содержит AH-заголовок (вложенное применение).

Протокол инкапсулирующей защиты ESP

Протокол инкапсулирующей защиты содержимого ESP обеспечивает конфиденциальность, аутентичность, целостность и защиту от повторов для пакетов данных. Следует отметить, что конфиденциальность данных протокол ESP обеспечивает всегда, а целостность и аутентичность являются для него опциональными требованиями. Конфиденциальность данных обеспечивается путем шифрования содержимого отдельных пакетов. Целостность и аутентичность данных обеспечиваются на основе вычисления дайджеста.

Из приведенного перечня функций по защите информационного обмена видно, что функциональность протокола ESP шире, чем протокола AH. Протокол ESP поддерживает все функции протокола AH по защите зашифрованных потоков данных от подлога, воспроизведения и случайного искажения, а также обеспечивает конфиденциальность данных.

В протоколе ESP функции аутентификации и криптографического закрытия могут быть задействованы либо вместе, либо отдельно друг от друга. При выполнении шифрования без аутентификации появляется возможность использования механизма трансляции сетевых адресов NAT, поскольку в этом случае адреса в заголовках IP-пакетов можно модифицировать [7].

Для решения своих задач протокол ESP использует заголовок формата, приведенного на рис. 9.11.

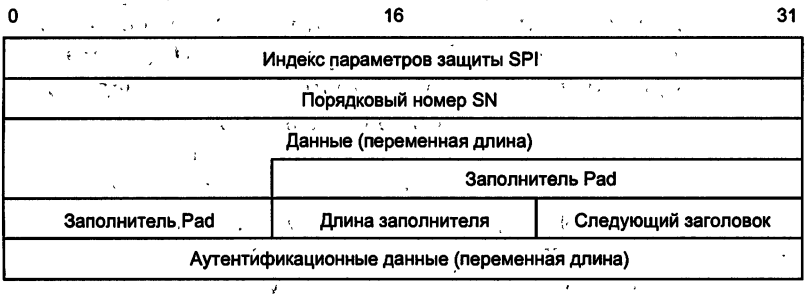


Рис. 9.11. Формат заголовка ESP

Заголовок ESP содержит следующие поля:

- *индекс параметров защиты SPI (Security Parameters Index)* — используется совместно с адресом получателя и протоколом защиты (AH или ESP). Указывает соответствующее соглашение SA. Получатель использует это значение для определения соглашения о защите, с которым идентифицируется этот пакет;
- *порядковый номер SN (Sequence Number)* — обеспечивает защиту от повторов для SA. Представляет собой 32-битное число, первоначально равное 1 и увеличивающееся с шагом 1. Оно не повторяется циклически и указывает номер пакета, отсылаемого по данному соглашению. Получатель проверяет это поле с целью удостовериться, что пакета с таким номером принято еще не было. Если же такой пакет уже был, он не принимается;
- *данные (Payload Data)*;
- *заполнитель (Padding)* — дописывается от 0 до 255 байт для 32-битного выравнивания с размером блока шифра;
- *длина заполнителя (Padding Length)* — указывает длину поля заполнителя в байтах;
- *следующий заголовок (Next Header)* — указывает природу передаваемых данных (например, TCP или UDP);
- *аутентификационные данные (Authentication Data)* — содержит код проверки целостности ICV и код аутентичности сообщения, используемые для проверки подлинности отправителя и целостности сообщения. Значение ICV вычисляется для заголовка ESP, передаваемых данных и концевой метки ESP. Поле Authentication Data помещается в заголовок ESP только при включенной аутентификации.

Нетрудно заметить, что некоторые поля заголовка ESP аналогичны полям заголовка AH: Next Header, SPI, SN, Authentication Data. Но имеется и два дополнительных поля — заполнитель (Padding) и длина заполнителя (Pad Length). Заполнитель может понадобиться в трех случаях. Во-первых, для нормальной работы некоторых алгоритмов шифрования необходимо, чтобы шифруемый текст содержал кратное число блоков определенного размера. Во-вторых, формат заголовка ESP требует, чтобы поле данных заканчивалось на границе четырех байтов. И наконец, заполнитель можно использовать для сокрытия действительного размера пакета в целях обеспечения так называемой частичной конфиденциальности трафика. Правда, протокол ESP ограничивает возможности маскировки 255 байтами заполнителя; это сделано для того, чтобы из-за большого объема избыточных данных не слишком снижалась полезная пропускная способность канала связи.

Как видно из рис. 9.11, заголовок делится на две части, разделяемые полем данных (полезная нагрузка — Payload Data). Первая часть, которая далее будет обозначаться как заголовок ESP, образуется двумя полями, SPI и SN, и размещается перед полем данных. Остальные служебные поля протокола ESP расположены в конце пакета. Непосредственно за полем данных следует так называемый трейлер, в который входят заполнитель (Padding), длина заполнителя (Pad Length), а также указатель на протокол следующего уровня (Next Header). Завершает пакет поле контроля целостности (Authentication Data). В том случае, когда при установлении безопасной ассоциации принято решение не использовать возможностей ESP по обеспечению целостности, это поле отсутствует.

Программное обеспечение перечисленных протоколов (утилиты шифрования, цифровой подписи и пр.) может функционировать на серверах или компьютерах конечных пользователей. Однако чаще его устанавливают на маршрутизаторах или специальных устройствах, которые в архитектуре IPSec именуются шлюзами безопасности (Security Gateway).

Различают два режима использования протокола ESP — транспортный и туннельный. На рис. 9.12 показано расположение ESP-заголовка в туннельном и транспортном режимах [63].

В *транспортном режиме* зашифрованные данные транспортируются непосредственно между хостами. В транспортном режиме протокола ESP заголовок исходного IP-пакета остается внешним. Заголовок ESP помещается в передаваемый пакет между заголовками протоколов третьего (IP) и четвертого (например, TCP) уровней. Заметим, что поля протокола ESP следуют после стандартного IP-заголовка, а это означает, что такой пакет может маршрутизироваться в сети с помощью обычного оборудования, поддерживающего IP.

Шифрованию подвергаются только данные исходного IP-пакета (пакет верхнего уровня) и заключительная часть ESP-заголовка (ESP trailer). В этом режиме ESP не шифрует заголовок IP-пакета, иначе маршрутизатор не сможет прочитать поля заголовка и корректно осуществить продвижение пакета между сетями. В число шифруемых по-

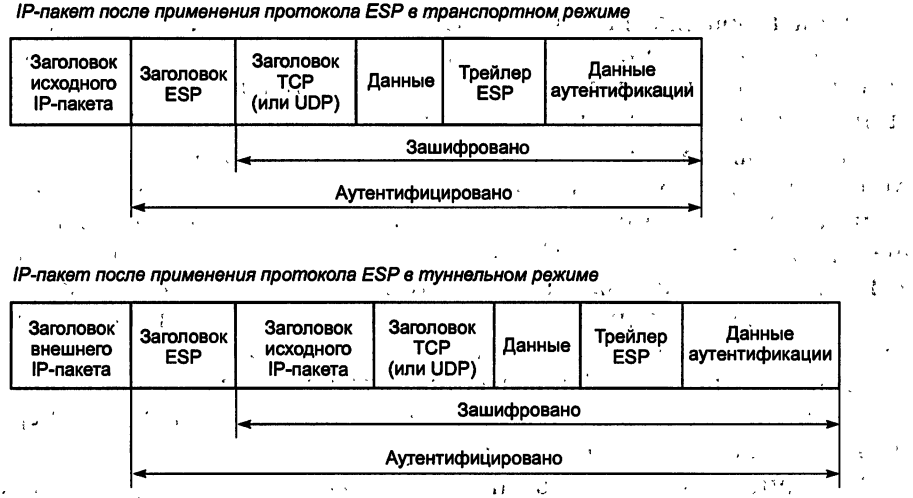


Рис. 9.12. IP-пакет после применения протокола ESP в транспортном и туннельном режимах

лей не попали также поля SPI и SN, которые должны передаваться в открытом виде для того, чтобы прибывший пакет можно было отнести к определенной ассоциации SA и защититься от ложного воспроизведения пакета.

В отличие от протокола AH, контроль целостности и аутентичности данных в протоколе ESP не распространяется на заголовок исходного пакета, и по этой причине имеет смысл применять оба протокола совместно — ESP для шифрования, а AH для контроля целостности.

Таким образом, адресная информация (IP-адреса отсылающей и принимающей сторон) видна при пересылке пакета по сети и несанкционированное изменение этих IP-адресов не будет замечено.

В *туннельном режиме* основная роль отводится шлюзам безопасности, поскольку предполагается, что клиентские станции (или серверы) могут не поддерживать IPSec и отправляют в сеть обычный IP-трафик. Перед тем как достичь каналов глобальной сети, каждый исходный IP-пакет сначала попадает в шлюз, который помещает этот пакет целиком в «оболочку» IPSec, зашифровывая его содержимое вместе с исходным IP-заголовком. Чтобы обеспечить возможность маршрутизации получившегося пакета, шлюз снабжает его новым IP-заголовком и только после этого отправляет в сеть. Шлюз, находящийся на противоположном конце соединения, расшифровывает этот пакет и передает его на оконечное устройство в первоначальном виде. Описанная процедура называется *туннелированием.*

Из рис. 9.12 видно, что в туннельном режиме в качестве внешнего заголовка создается новый заголовок IP. Весь исходный IP-пакет (и данные, и заголовок IP) и заключительная часть заголовка ESP (трейлер ESP) шифруются. Поэтому адресная информация исходного IP-пакета недоступна для просмотра. Заголовок внешнего IP-пакета протоколом ESP не защищается.

Туннелирование позволяет распространить действие средств защиты на сетевой уровень модели OSI и, в частности, скрыть истинные адреса источника и получателя. При этом уменьшается риск атак, основанных на детальном анализе трафика.

Сравнивая протоколы ESP и AH, можно заметить, что они дублируют функциональность друг друга в области обеспечения аутентификации данных. Главным отличием протокола AH от ESP в данном вопросе является то, что протокол AH обеспечивает аутентификацию всего пакета (и IP-заголовка и самих данных), в то время как протокол ESP аутентифицирует только данные из пакета (см. рис. 9.12). При шифровании в протоколе ESP используется симметричный секретный ключ, т. е. передаваемые данные зашифровываются и расшифровываются с помощью одного и того же ключа. Для протокола ESP также определен перечень обязательных алгоритмов шифрования — это DES, MD5 и SHA-1.

При аутентификации данных протокол ESP использует те же алгоритмы HMAC, что и протокол AH (использующие MD5 или SHA-1 в качестве функции хэширования). Однако способы применения различаются (см. рис. 9.12):

- в транспортном режиме протокол ESP аутентифицирует только данные из пакета, не затрагивая IP-заголовка (протокол AH в том же режиме защищает и данные и оба заголовка);
- в туннельном режиме аутентификация в ESP протоколе применяется к данным пакета и исходному IP-заголовку, но не затрагивает новый IP-заголовок (протокол AH в туннельном режиме аутентифицирует данные, AH-заголовок и оба IP-заголовка).

Протокол ESP может применяться отдельно или совместно с протоколом AH. При совместном использовании протоколы AH и ESP могут комбинироваться разными способами. Если используется транспортный режим, то аналогично тому, как в рамках ESP аутентификация идет следом за шифрованием, протокол AH должен применяться после протокола ESP. В туннельном режиме протоколы AH и ESP применяются к разным вложенным пакетам и, кроме того, допускается многократная вложенность туннелей с различными начальными и/или конечными точками.

Алгоритмы аутентификации и шифрования в IPSec

Стек протоколов IPSec представляет собой согласованный набор открытых стандартов, имеющий вполне определенное ядро, и в то же время он может быть достаточно просто дополнен новыми протоколами, алгоритмами и функциями. Благодаря модульной структуре протоколы AH и ESP допускают применение пользователями по их согласованному выбору различных криптографических алгоритмов аутентификации и шифрования. Для шифрования данных в IPSec (протокол ESP) может быть применен практически любой симметричный алгоритм шифрования, использующий секретные ключи.

Для обеспечения целостности и аутентификации данных (протоколы AH и ESP) используется один из приемов шифрования — шифрование с помощью односторонней функции (One-way Function), называемой также хэш-функцией (Hash Function) или дайджест-функцией (Digest Function) [41, 73]. Эта функция, примененная к шифруемым данным, дает в результате дайджест-значение, состоящее из фиксированного небольшого числа байтов. Дайджест передается в IP-пакете вместе с исходным сообщением. Получатель, зная, какая односторонняя функция шифрования была применена для составления дайджеста, заново вычисляет его, используя исходное сообщение. Если значения полученного и вычисленного дайджестов совпадают, это значит, что содержимое пакета во время передачи не было подвергнуто никаким изменениям. Знание дайджеста не дает возможности восстановить исходное сообщение и поэтому не может быть использовано для защиты конфиденциальности, но зато оно позволяет проверить целостность данных.

Дайджест является своего рода контрольной суммой для исходного сообщения. В отличие от традиционной контрольной суммы, при вычислении дайджеста используется секретный ключ. Если для получения дайджеста применялась односторонняя функция с параметром (в качестве которого выступает секретный ключ), известным только отправителю и получателю, любая модификация исходного сообщения будет немедленно обнаружена.

В целях обеспечения совместимости продуктов разных производителей рабочая группа IETF определила базовый набор поддерживаемых функций и алгоритмов, который должен быть однотипно реализован во всех продуктах, поддерживающих IPSec. На сегодня определены два алгоритма аутентификации и семь алгоритмов шифрования.

В настоящий момент для протоколов AH и ESP зарегистрировано два алгоритма аутентификации — HMAC-MD5 и HMAC-SHA-1. Алгоритм HMAC (Keyed-Hashing for Message Authentication Code) определяется стандартом RFC 2104. Функции MD5 (Message Digest version 5, стандарт RFC 1321) и SHA-1 (Secure Hash Algorithm version 1, стандарт FIPS 180-1) являются функциями хэширования. Алгоритмы HMAC-MD5 и HMAC-SHA-1 являются алгоритмами аутентификации с общим секретным ключом. Секретный ключ имеет длину 128 бит в случае MD5 и 160 бит в случае SHA-1 [7].

Если секретный ключ известен только передающей и принимающей сторонам, это обеспечит аутентификацию источника данных, а также целостность пакетов, пересылаемых между двумя сторонами. Для обеспечения совместимости оборудования и программного обеспечения на начальной стадии реализации протокола IPSec один из зарегистрированных алгоритмов аутентификации принято использовать по умолчанию. В качестве такого алгоритма определен алгоритм HMAC-MD5.

Структура алгоритма HMAC показана на рис. 9.13. Принцип действия алгоритма HMAC заключается в двукратной обработке пакета функцией хэширования, управляемой ключом аутентификации (например, функцией хэширования MD5).

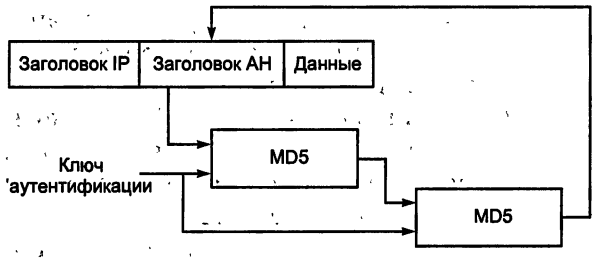


Рис. 9.13. Структура HMAC-алгоритма

Как видно из рис. 9.13, оба раза в обрабатываемые данные включается секретный ключ, который обеспечивает аутентификацию передаваемой информации. Полученная контрольная сумма помещается в заголовок протокола AH. Проверка аутентификации на другой стороне осуществляется путем повторного вычисления контрольной суммы для пришедшего пакета с использованием такого же ключа и сравнении полученного результата с присланным.

HMAC — это алгоритм аутентификации с секретным ключом. Целостность данных и аутентификация их источника, обеспечиваемые им, зависят от масштаба распространения секретного ключа. Если ключ HMAC известен только передающей и принимающей сторонам, это обеспечит и аутентификацию источника данных, и целостность пакетов данных, пересылаемых между двумя сторонами. Ключи для HMAC генерируются посредством процедуры ISAKMP/Oakley.

Алгоритм HMAC реализует симметричную схему аутентификации, используя параметр проверки целостности пакета ICV (Integrity Check Value). По сути, он представляет собой цифровую подпись, помещаемую в поле аутентификации и позволяющую отправителю подписать результат предварительного хэширования содержательной части пакета ESP.

Анализ содержимого этого поля дает возможность получателю идентифицировать источник данных и убедиться в том, что они не были изменены в процессе передачи. Если для протокола ESP функции аутентификации являются факультативными, то для протокола AH процесс аутентификации является обязательным.

Для протокола ESP зарегистрировано несколько алгоритмов шифрования. Чаще всего в качестве алгоритмов шифрования для ESP применяются DES (Data Encryption Standard), 3-DES (тройной DES) и новый стандарт шифрования AES (Advanced Encryption Standard). Для обеспечения IPSec-совместимости по умолчанию в качестве алгоритма шифрования стандартом предусмотрен симметричный метод DES-CBC (Cipher Block Chaining) с явно заданным вектором инициализации IV и с 56-разрядным ключом. Алгоритм AES повсюду встраивается в стандарт IPSec как альтернатива DES и 3-DES.

Выбор алгоритма шифрования целиком зависит от разработчика. Возможность выбора алгоритма шифрования предоставляет пользователю дополнительное преимущество: ведь злоумышленник должен не только вскрыть шифр, но и определить, какой именно шифр ему надо

вскрывать. Вместе с необходимостью подбора ключей это еще более уменьшает шансы злоумышленника своевременно расшифровать данные пользователя.

IPSec может работать совместно с протоколами L2TP или L2F, которые выполняют только туннелирование, но не обеспечивают шифрование и аутентификацию данных. Эти протоколы создают через Интернет туннель для пакетов любых протоколов, упаковывая их в пакеты IP. Когда трафик с помощью L2F или L2TP оказывается упакованным в пакеты IP, то дальше для его защиты можно использовать IPSec. В результате комбинирование IPSec с протоколами туннелирования типа L2F/L2TP позволяет решить задачу защиты данных для протоколов, отличных от IP.

Алгоритмическая независимость протоколов AH и ESP требует предварительного согласования взаимодействующими сторонами набора применяемых алгоритмов и их параметров.

9.2.3. Протокол управления криптоключами IKE

Протоколы ESP и AH позволяют реализовать важнейшие атрибуты защищенной передачи — конфиденциальность связи, аутентификацию сторон и целостность данных. Однако их функции теряют всякую ценность в отсутствие мощной поддерживающей инфраструктуры, которая обеспечивала бы распределение ключей и согласование протоколов между участниками обмена.

Роль такой инфраструктуры в IPSec выполняет группа протоколов *IKE (Internet KeyExchange)*. Это название пришло в 1998 г. на смену более раннему — ISAKMP/Oakley, которое непосредственно указывало на происхождение средств управления ключами в составе IPSec.

Протокол *ISAKMP (Internet Security Association and Key Management Protocol),* описанный в документе RFC 2408, позволяет согласовывать алгоритмы и математические структуры (так называемые мультипликативные группы, определенные на конечном поле) для процедуры обмена ключами Диффи — Хеллмана, а также процессов аутентификации [7, 63]. Протокол Oakley, описанный в RFC 2412, основан на алгоритме Диффи — Хеллмана и служит для организации непосредственного обмена ключами.

Протоколы IKE решают три задачи:

- осуществляют аутентификацию взаимодействующих сторон, согласовывают алгоритмы шифрования и характеристики ключей, которые будут использоваться в защищенном сеансе обмена информацией;
- обеспечивают создание ключевой информации соединения и управление ею, непосредственный обмен ключами (в том числе возможность их частой смены);
- управляют параметрами соединения и защитой от некоторых типов атак, контролируют выполнение всех достигнутых соглашений.

Разработчики IPSec начали свою деятельность с решения последней из перечисленных задач. В результате на свет появилась *концепция защищенных виртуальных соединений* или *безопасных ассоциаций SA (Security Associations)*.

Установление безопасной ассоциации

Основой функционирования IPSec являются защищенные виртуальные соединения, или безопасные ассоциации SA. Для того чтобы протоколы AH и ESP могли выполнять свою работу по защите передаваемых данных, между двумя конечными точками должна быть сформирована ассоциация SA. Безопасная ассоциация SA представляет собой соглашение о защите обмена данными между двумя взаимодействующими партнерами.

Установление безопасной ассоциации SA должно начинаться со взаимной аутентификации сторон, потому что меры безопасности теряют всякий смысл, если данные передаются или принимаются неавторизованными пользователями. Процедуры установления безопасной ассоциации SA оправданны лишь в том случае, если у каждой из сторон имеется полная уверенность в том, что ее партнер — именно тот, за кого он себя выдает.

Для выполнения аутентификации сторон в IKE применяются два основных способа.

Первый способ основан на использовании разделяемого секрета. Перед инициализацией IPSec-устройств, образующих безопасные ассоциации, в их базу данных помещается предварительно распределенный разделяемый секрет. Цифровая подпись на основе односторонней функции, например MD5, использующей в качестве аргумента этот предварительно распределенный секрет, доказывает аутентичность противоположной стороны.

Второй способ основан на использовании технологии цифровой подписи и цифровых сертификатов стандарта X.509: каждая из сторон подписывает свой цифровой сертификат своим закрытым ключом и передает эти данные противоположной стороне. Если подписанный сертификат расшифровывается открытым ключом отправителя, то это удостоверяет тот факт, что отправитель, предоставивший данные, действительно обладает ответной частью данного открытого ключа — соответствующим закрытым ключом.

Однако следует отметить, что для удостоверения аутентичности стороны нужно еще убедиться в аутентичности самого сертификата, и для этого сертификат должен быть подписан не только его владельцем, но и некоторой третьей стороной, выдавшей сертификат и вызывающей доверие. В архитектуре IPSec эта третья сторона именуется органом сертификации CA (Certification Authority).

После проведения взаимной аутентификации взаимодействующие стороны могут непосредственно перейти к согласованию параметров за-

щищенного канала. Выбираемые параметры безопасной ассоциации SA определяют протокол, используемый для обеспечения безопасности передачи данных; алгоритм аутентификации протокола AH и его ключи; алгоритм шифрования, используемый протоколом ESP, и его ключи; наличие или отсутствие криптографической синхронизации; способы защиты сеанса обмена; частоту смены ключей и ряд других параметров. Важным параметром безопасной ассоциации SA является так называемый криптографический материал, т. е. секретные ключи, используемые в работе протоколов AH и ESP. Сервисы безопасности, предлагаемые IPSec, используют для формирования криптографических ключей разделяемые секреты.

Параметры безопасной ассоциации SA должны устраивать обе конечные точки защищенного канала. Поэтому при использовании автоматической процедуры установления SA протоколы IKE, работающие по разные стороны канала, выбирают параметры в ходе переговорного процесса. Безопасная ассоциация SA представляет собой в IPSec однонаправленное логическое соединение, поэтому при двустороннем обмене данными необходимо установить две ассоциации SA. В рамках одной ассоциации SA может работать только один из протоколов защиты данных — либо AH, либо ESP, но не оба вместе.

Система IPSec допускает применение ручного и автоматического способов установления безопасной ассоциации.

Базы данных SAD и SPD

В каждом узле, поддерживающем IPSec, используются базы данных двух типов:

- база данных безопасных ассоциаций SAD (Security Associations Database);
- база данных политики безопасности SPD (Security Policy Database).

При установлении безопасной ассоциации SA две вступающие в обмен стороны принимают ряд соглашений, регламентирующих процесс передачи потока данных между ними. Соглашения представляются в виде набора параметров. Для безопасной ассоциации SA такими параметрами являются, в частности, тип и режим работы протокола защиты (AH или ESP), методы шифрования, секретные ключи, значение текущего номера пакета в ассоциации и другая информация.

Наборы текущих параметров, определяющих все активные ассоциации, хранятся на обоих оконечных узлах защищенного канала в виде баз данных безопасных ассоциаций SAD. Каждый узел IPSec поддерживает две базы SAD: одну для исходящих ассоциаций, а другую для входящих.

Кроме базы данных безопасных ассоциаций SAD в архитектуре IPSec существует еще один компонент — база данных политики безопасности SPD, которая задает соответствие между IP-пакетами и уста-

новленными для них правилами обработки. При обработке пакетов базы данных SPD используются совместно с базами данных SAD. База данных политики безопасности SPD представляет собой упорядоченный набор правил, каждое из которых включает совокупность селекторов и допустимых политик безопасности. Селекторы служат для отбора пакетов, а политики безопасности задают требуемую обработку. Такая база данных формируется и поддерживается на каждом узле, где установлено программное обеспечение IPSec.

Политика безопасности предусматривает три возможных варианта обработки IP-пакета:

- отбрасывание пакета;
- передача пакета без изменения;
- обработка средствами IPSec.

Каждый узел IPSec должен поддерживать две базы SPD: одну для исходящего трафика, а другую для входящего, так как может требоваться разная защита в разных направлениях.

Использование баз SPD и SAD для управления процессом защиты трафика позволяет достаточно гибко сочетать механизм безопасных ассоциаций, который предусматривает установление логического соединения, с дейтаграммным характером трафика протокола IP. Соответствующая настройка базы SDP позволяет выбирать нужную степень детализации защиты — от применения одной общей ассоциации для трафика большого количества конечных узлов до защиты каждого отдельного приложения с помощью индивидуально настроенной ассоциации.

Согласование параметров защищенных каналов и распределение криптографических ключей

При построении защищенных виртуальных сетей VPN важную роль играют функции согласования параметров защищенных туннелей и распределения криптографических ключей. Эти функции должны реализовываться при формировании каждого криптозащищенного канала.

Применяемые в VPN криптографические ключи можно разделить по длительности использования на следующие типы:

- основные ключи, которые применяются в течение относительно долгого периода времени (от недели до нескольких месяцев);
- временные ключи, каждый из которых генерируется для криптозащиты информации в рамках одного защищенного канала.

Основные ключи обеспечивают аутентификацию сторон, а также криптозащиту распределяемых временных ключей. Основные ключи должны распределяться заблаговременно до формирования защищенных виртуальных соединений. Наиболее высокая эффективность распределения основных криптографических ключей достигается при использовании асимметричных криптосистем, когда распределению подлежат только открытые ключи.

Временные (сеансовые) ключи, действующие в рамках одного криптозащищенного туннеля, распределяются по сети с помощью основных ключей. Одним из наиболее популярных алгоритмов формирования сеансового ключа на основе распределенных или передаваемых друг другу открытых ключей является алгоритм Диффи — Хеллмана. Поскольку для шифрования передаваемых данных используются симметричные криптосистемы, сеансовые ключи, как правило, являются симметричными ключами шифрования.

После аутентификации сторон и безопасного распределения временных ключей, а также согласования параметров защищенного туннеля криптозащита трафика в рамках этого туннеля осуществляется на основе распределенных временных ключей.

Существует два основных способа построения защищенного виртуального туннеля между двумя узлами компьютерной сети:

- формирование защищенного канала для каждого соединения, устанавливаемого каким-либо программным приложением;
- формирование общего защищенного канала между сетевыми узлами и создание в рамках этого канала отдельных защищенных соединений [63].

Формирование защищенного виртуального канала для каждого соединения включает следующие этапы:

- выдачу запроса одной из сторон и достижение соглашения на создание защищенного виртуального канала;
- аутентификацию сторон, выполняемую с помощью ранее распределенных основных ключей шифрования или назначенных паролей;
- распределение временных ключей и согласование параметров защищенного канала.

Обычно второй и третий этапы совмещаются друг с другом и аутентификация выполняется совместно с распределением временных ключей.

При формировании между двумя сетевыми узлами общего защищенного канала, в рамках которого затем создаются отдельные защищенные соединения, перечисленные этапы выполняются как при установлении защищенного канала, так и при создании каждого защищенного соединения.

В начале формирования общего защищенного канала распределяется главный сеансовый ключ симметричного шифрования. Это распределение осуществляется с помощью основных ключей взаимодействующих сторон. Распределение же временных ключей для каждого создаваемого защищенного соединения выполняется на основе главного сеансового ключа. Независимо от числа защищенных соединений, создаваемых в рамках одного защищенного туннеля, основные ключи используются только один раз — при распределении главного сеансового ключа.

Способ формирования общего защищенного канала и создания затем на его основе отдельных защищенных соединений характеризуется

более высокой сложностью реализации. Однако в этом случае снижается уязвимость закрытых основных ключей, служащих для распределения главного сеансового ключа, и может быть обеспечено более эффективное расходование компьютерных ресурсов, затрачиваемых на генерацию временных ключей.

Процесс установления защищенного соединения в протоколе IKE разбит на две фазы. Во время *первой фазы* происходит аутентификация участников, стороны договариваются о том, как они будут защищать обмен информацией во второй фазе, и происходит выработка ключевого материала для защиты обменов во второй фазе.

Во *второй фазе* участники договариваются о параметрах защищенного соединения (какие алгоритмы и в каком порядке использовать, параметры этих алгоритмов и т. п.) и обмениваются ключевой информацией (хотя это действие опционально). Все обмены второй фазы и часть обменов первой фазы передаются в зашифрованном виде (о том, как и чем шифровать, стороны договариваются в первой фазе) [7].

9.2.4. Особенности реализации средств IPSec

Протоколы AH или ESP могут защищать передаваемые данные в двух режимах:

- туннельном, при котором IP-пакеты защищаются целиком, включая их заголовки;
- транспортном, обеспечивающем защиту только содержимого IP-пакетов.

Основным режимом является туннельный. В туннельном режиме исходный пакет помещается в новый IP-пакет и передача данных по сети выполняется на основании заголовка нового IP-пакета.

При работе в этом режиме каждый обычный IP-пакет помещается целиком в криптозащищенном виде в конверт IPSec, а тот, в свою очередь, инкапсулируется в другой защищенный IP-пакет. Туннельный режим обычно реализуют на специально выделенных шлюзах безопасности, в роли которых могут выступать маршрутизаторы или межсетевые экраны. Между такими шлюзами и формируются защищенные туннели IPSec.

После приема на другой стороне туннеля защищенные IP-пакеты распаковываются и полученные исходные IP-пакеты передаются компьютерам приемной локальной сети по стандартным правилам. В транспортном режиме передача IP-пакета через сеть выполняется с помощью исходного заголовка этого пакета. В конверт IPSec в криптозащищенном виде помещается только содержимое исходного IP-пакета, и к полученному конверту добавляется исходный IP-заголовок. Транспортный режим быстрее туннельного и разработан для применения на оконечных системах. Данный режим может использоваться для поддержки удаленных и мобильных пользователей, а также для защиты информационных потоков внутри локальных сетей.

Основные схемы применения IPSec

Применение туннельного или транспортного режима зависит от требований, предъявляемых к защите данных, а также от роли узла, в котором работает IPSec. Узлом, завершающим защищенный канал, может быть *хост* (конечный узел) или *шлюз* (промежуточный узел) [42]. Соответственно различают три основные схемы применения IPSec: хост—хост, шлюз—шлюз и хост—шлюз.

В первой схеме защищенный канал, или, что в данном контексте одно и то же, безопасная ассоциация, устанавливается между двумя конечными узлами сети, т. е. хостами H1 и H2 (рис. 9.14). Протокол IPSec в этом случае работает на конечном узле и защищает данные, поступающие на него. Для хостов, поддерживающих IPSec, разрешается использовать как транспортный режим, так и туннельный.

Рис. 9.14. Схема хост—хост

В соответствии со второй схемой защищенный канал устанавливается между двумя промежуточными узлами, называемыми шлюзами безопасности SG1 и SG2, на каждом из которых работает протокол IPSec (рис. 9.15).

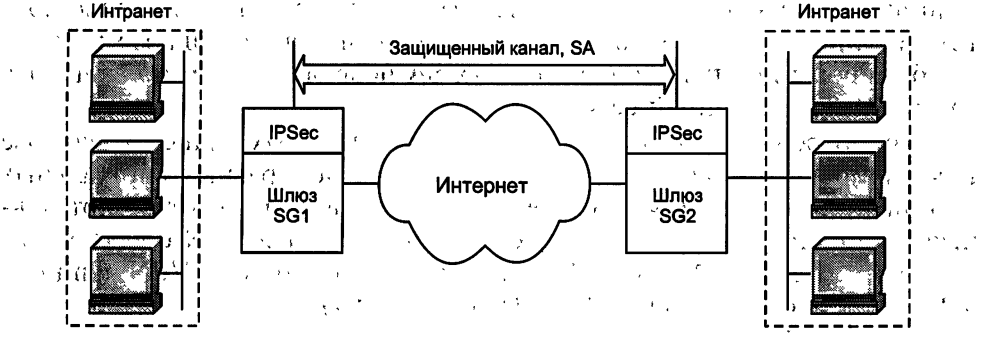


Рис. 9.15. Схема шлюз—шлюз

Шлюз безопасности представляет собой сетевое устройство, подключаемое к двум сетям, которое выполняет функции шифрования и аутентификации для хостов, расположенных позади него. Шлюз безопасности VPN может быть реализован в виде отдельного программного продукта, отдельного аппаратного устройства, а также в виде маршрутизатора или межсетевого экрана, дополненного функциями VPN.

Защищенный обмен данными может происходить между любыми двумя конечными узлами, подключенными к сетям, которые расположены позади шлюзов безопасности. При защищенном удаленном доступе часто применяется схема хост—шлюз (рис. 9.16).

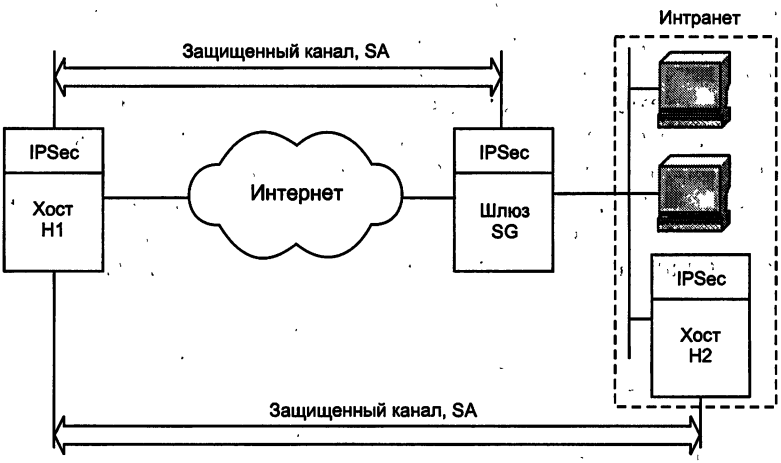


Рис. 9.16. Схема хост—шлюз, дополненная каналом хост—хост

Здесь защищенный канал организуется между удаленным хостом H1, на котором работает IPSec, и шлюзом SG, защищающим трафик для всех хостов, входящих в сеть Intranet предприятия. Удаленный хост может использовать при отправке пакетов шлюзу как транспортный, так и туннельный режим, шлюз же отправляет пакеты хосту только в туннельном режиме.

Эту схему можно модифицировать, создав параллельно еще один защищенный канал — между удаленным хостом H1 и каким-либо хостом H2, принадлежащим внутренней сети, защищаемой шлюзом. Такое комбинированное использование двух SA позволяет надежно защитить трафик и во внутренней сети.

Рассмотренные схемы построения защищенных каналов на базе IPSec широко применяются при создании разнообразных виртуальных защищенных сетей VPN. На базе IPSec успешно реализуются виртуальные защищенные сети любой архитектуры, включая VPN с удаленным доступом (Remote Access VPN), внутрикорпоративные VPN (Intranet VPN) и межкорпоративные VPN (Extranet VPN).

Преимущества средств безопасности IPSec

Система стандартов IPSec вобрала в себя прогрессивные методики и достижения в области сетевой безопасности, завоевала признание специалистов как надежная и легко интегрируемая система безопасности для IP-сетей. Система IPSec прочно занимает лидирующие позиции в наборе стандартов для создания VPN. Этому способствует ее открытое

построение, способное включать все новые достижения в области криптографии. IPsec позволяет защитить сеть от большинства сетевых атак, «сбрасывая» чужие пакеты еще до того, как они достигнут уровня IP на принимающем компьютере. В защищаемый компьютер или сеть могут войти только пакеты от зарегистрированных партнеров по взаимодействию.

IPsec обеспечивает:

- аутентификацию — доказательство отправки пакетов вашим партнером по взаимодействию, т. е. обладателем разделяемого секрета;
- целостность — невозможность изменения данных в пакете;
- конфиденциальность — невозможность раскрытия передаваемых данных;
- надежное управление ключами — протокол IKE вычисляет разделяемый секрет, известный только получателю и отправителю пакета;
- туннелирование — полную маскировку топологии локальной сети предприятия.

Работа в рамках стандартов IPSec обеспечивает полную защиту информационного потока данных от отправителя до получателя, закрывая трафик для наблюдателей на промежуточных узлах сети. VPN-решения на основе стека протоколов IPSec обеспечивают построение виртуальных защищенных сетей, их безопасную эксплуатацию и интеграцию с открытыми коммуникационными системами.

9.3. Защита на сеансовом уровне — протоколы SSL/TLS и SOCKS

Самым высоким уровнем модели OSI, на котором возможно формирование защищенных виртуальных каналов, является пятый — сеансовый уровень. При построении защищенных виртуальных сетей на сеансовом уровне появляется возможность криптографической защиты информационного обмена, включая аутентификацию, а также реализацию ряда функций посредничества между взаимодействующими сторонами.

Действительно, сеансовый уровень модели OSI отвечает за установку логических соединений и управление этими соединениями. Поэтому существует возможность применения на этом уровне программ-посредников, проверяющих допустимость запрошенных соединений и обеспечивающих выполнение других функций защиты межсетевого взаимодействия.

Протоколы формирования защищенных виртуальных каналов на сеансовом уровне прозрачны для прикладных протоколов защиты, а также высокоуровневых протоколов предоставления различных сервисов (протоколов HTTP, FTP, POP3, SMTP и др.). Однако на сеансовом

уровне начинается непосредственная зависимость от приложений, реализующих высокоуровневые протоколы. Поэтому реализация протоколов защиты информационного обмена, соответствующих этому уровню, в большинстве случаев требует внесения изменений в высокоуровневые сетевые приложения.

Для защиты информационного обмена на сеансовом уровне широкое распространение получил протокол SSL. Для выполнения на сеансовом уровне функций посредничества между взаимодействующими сторонами организацией IETF (Internet Engineering Task Force) в качестве стандарта принят протокол SOCKS [7].

9.3.1. Протоколы SSL/TLS

Протокол SSL (Secure Socket Layer — протокол защищенных сокетов) был разработан компанией Netscape Communications совместно с RSA Data Security для реализации защищенного обмена информацией в клиент/серверных приложениях. В настоящее время протокол SSL применяется в качестве протокола защищенного канала, работающего на сеансовом уровне модели OSI.

Протокол SSL использует криптографические методы защиты информации для обеспечения безопасности информационного обмена. Этот протокол выполняет все функции по созданию защищенного канала между двумя абонентами сети, включая их взаимную аутентификацию, обеспечение конфиденциальности, целостности и аутентичности передаваемых данных. Ядром протокола SSL является технология комплексного использования асимметричных и симметричных криптосистем.

Взаимная аутентификация обеих сторон в SSL выполняется путем обмена цифровыми сертификатами открытых ключей пользователей (клиента и сервера), заверенными цифровой подписью специальных сертификационных центров. Протокол SSL поддерживает сертификаты, соответствующие общепринятому стандарту X.509, а также стандарты инфраструктуры открытых ключей PKI (Public Key Infrastructure), с помощью которой организуется выдача и проверка подлинности сертификатов.

Конфиденциальность обеспечивается шифрованием передаваемых сообщений с использованием симметричных сессионных ключей, которыми стороны обмениваются при установлении соединения. Сессионные ключи передаются также в зашифрованном виде, при этом они шифруются с помощью открытых ключей, извлеченных из сертификатов абонентов. Использование для защиты сообщений симметричных ключей связано с тем, что скорость процессов шифрования и расшифрования на основе симметричного ключа существенно выше, чем при использовании несимметричных ключей.

Подлинность и целостность циркулирующей информации обеспечивается за счет формирования и проверки электронной цифровой

подписи. Для цифровых подписей и обмена ключами шифрования используются алгоритмы с открытым ключом.

В качестве алгоритмов асимметричного шифрования используются алгоритм RSA, а также алгоритм Диффи — Хеллмана. Допустимыми алгоритмами симметричного шифрования являются RC2, RC4, DES, 3-DES и AES. Для вычисления хэш-функций могут применяться стандарты MD5 и SHA-1. В протоколе SSL версии 3.0 набор криптографических алгоритмов является расширяемым.

Согласно протоколу SSL криптозащищенные туннели создаются между конечными точками виртуальной сети. Инициаторами каждого защищенного туннеля являются клиент и сервер, функционирующие на компьютерах в конечных точках туннеля (рис. 9.17).

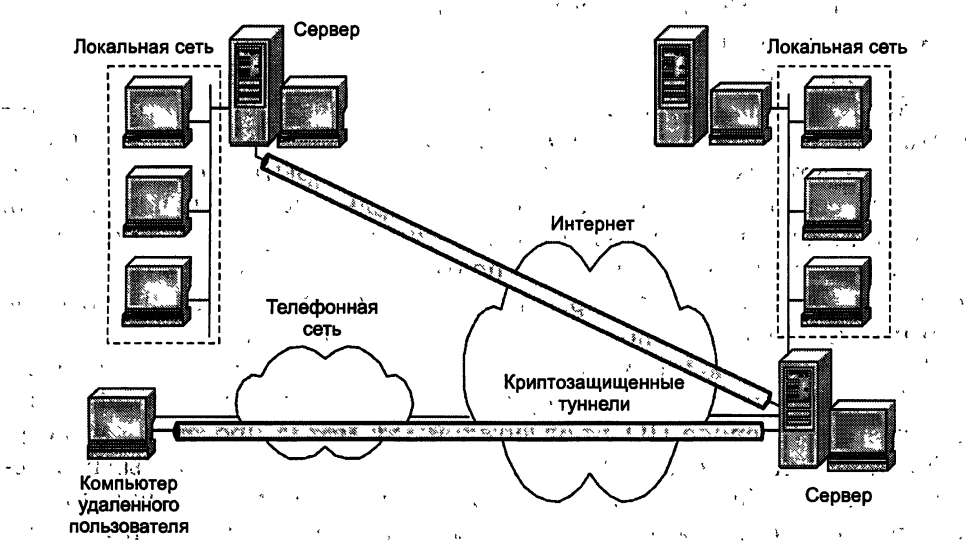


Рис. 9.17. Криптозащищенные туннели, сформированные на основе протокола SSL

Протокол SSL предусматривает следующие этапы взаимодействия клиента и сервера при формировании и поддержке защищаемого соединения:

- установление SSL-сессии;
- защищенное взаимодействие.

В процессе установления SSL-сессии решаются следующие задачи:

- аутентификация сторон;
- согласование криптографических алгоритмов и алгоритмов сжатия, которые будут использоваться при защищенном информационном обмене;
- формирование общего секретного мастер-ключа;
- генерация на основе сформированного мастер-ключа общих секретных сеансовых ключей для криптозащиты информационного обмена [7, 68].

Процедура установления SSL-сессии, называемая также процедурой рукопожатия, отрабатывается перед непосредственной защитой инфор-

мационного обмена и выполняется по протоколу начального приветствия (Handshake Protocol), входящему в состав протокола SSL.

При установлении повторных соединений между клиентом и сервером стороны могут, по взаимному соглашению, формировать новые сеансовые ключи на основе старого общего секрета (данная процедура называется продолжением SSL-сессии).

В реализациях протокола SSL для аутентификации взаимодействующих сторон и формирования общих секретных ключей чаще всего используют алгоритм RSA.

Соответствие между открытыми ключами и их владельцами устанавливается с помощью цифровых сертификатов, выдаваемых специальными центрами сертификации (см. главу 4).

В протоколе SSL предусмотрены два типа аутентификации:

- аутентификация сервера клиентом;
- аутентификация клиента сервером.

SSL-аутентификация сервера позволяет клиенту проверить подлинность сервера. Клиентское ПО, поддерживающее SSL, может с помощью стандартных приемов криптографии с открытым ключом проверить, что сертификат сервера и открытый ключ действительны и были выданы источником, находящимся в списке доверенных источников сертификатов этого клиента. Это подтверждение может быть важным, если пользователь, например, отправляет номер кредитной карты по сети и хочет проверить подлинность сервера-получателя.

SSL-аутентификация клиента позволяет серверу проверить личность пользователя. Используя те же приемы, что и в случае с аутентификацией сервера, серверное ПО с поддержкой SSL может проверить, что сертификат клиента и открытый ключ действительны и были выданы источником сертификатов, имеющимся в списке доверенных источников сервера. Это подтверждение может быть важным, если, например, сервер — это банк, отправляющий конфиденциальную финансовую информацию заказчику, и он хочет проверить личность получателя. Процесс аутентификации клиента сервером иллюстрируется рис. 9.18.

Процедуры формирования общего секретного мастер-ключа и генерации на основе сформированного мастер-ключа общих секретных сеансовых ключей для криптозащиты информационного обмена рассмотрены в главе 5.

Протокол SSL прошел проверку временем, работая в популярных браузерах Netscape Navigator и Internet Explorer, а также на веб-серверах ведущих производителей. В 1999 г. на смену версии SSL 3.0 пришел протокол TLS (Transport Layer Security), который базируется на протоколе SSL и в настоящее время является стандартом Интернета.

Различия между протоколами SSL 3.0 и TLS 1.0 не слишком существенны. Спецификации SSL были в свое время предложены в качестве официальных стандартов Интернета, но не получили этого статуса по формальным обстоятельствам. Протокол SSL стал промышленным протоколом, развиваемым и продвигаемым вне технических координирующих институтов Интернета.

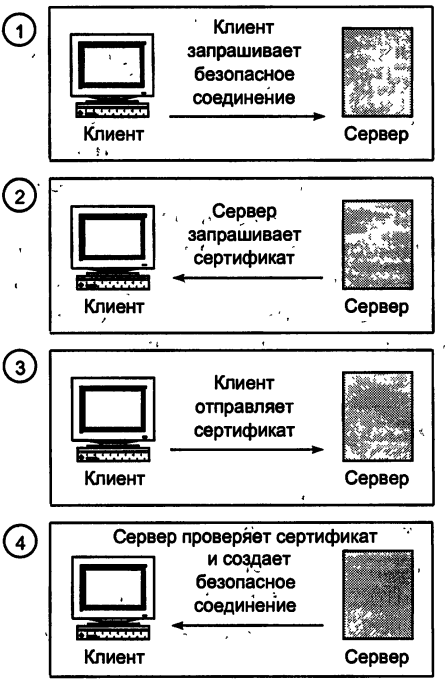


Рис. 9.18. Процесс аутентификации клиента сервером

Некоторые *функции безопасности*, предоставляемые протоколом SSL:

- шифрование данных с целью предотвратить раскрытие конфиденциальных данных во время передачи;
- подписывание данных с целью предотвратить несанкционированное изменение данных во время передачи;
- аутентификация клиента и сервера, позволяющая убедиться, что общение ведется с соответствующим человеком или компьютером.

Протокол SSL поддерживается программным обеспечением серверов и клиентов, выпускаемых ведущими западными компаниями. Существенным недостатком протокола SSL является то, что практически все продукты, поддерживающие SSL, из-за экспортных ограничений доступны за пределами США лишь в усеченном варианте. Следует отметить, что последние экспортные релизы этих продуктов все же поддерживают ряд алгоритмов с достаточной длиной ключа, но с особыми ограничениями. Возникают также трудности создания и использования национальных центров сертификации.

К недостаткам протоколов SSL и TLS можно отнести то, что для транспортировки своих сообщений они используют только один протокол сетевого уровня — IP — и, следовательно, могут работать только в IP-сетях. Кроме того, применение на практике защитных свойств SSL/TLS не в полной мере прозрачно для прикладных протоколов.

Еще одним негативным моментом в SSL являются возобновляемые сессии, суть которых заключается в том, что, если клиент и сервер разорвали соединение, они могут возобновить его, проведя минимальный

обмен данными, и использовать старый параметр SessionID. Злоумышленник, скомпрометировав одну из предыдущих сессий, может провести с сервером процедуру ее восстановления. В результате будут скомпрометированы все последующие данные, передаваемые в данной сессии.

Кроме того, в SSL для аутентификации и шифрования используются одинаковые ключи, что при определенных условиях может привести к потенциальной уязвимости. Подобное решение дает возможность собрать больше статистического материала, чем при аутентификации и шифровании разными ключами. Как и другие программные продукты, SSL подвержен атакам, связанным с недоверенной программной средой, внедрением программ-закладок и др.

9.3.2. Протокол SOCKS

Протокол SOCKS организует процедуру взаимодействия клиент/серверных приложений на сеансовом уровне модели OSI через сервер-посредник, или прокси-сервер [7].

В общем случае программы-посредники, которые традиционно используются в межсетевых экранах, могут выполнять следующие функции:

- идентификацию и аутентификацию пользователей;
- криптозащиту передаваемых данных;
- разграничение доступа к ресурсам внутренней сети;
- разграничение доступа к ресурсам внешней сети;
- фильтрацию и преобразование потока сообщений, например поиск вирусов и прозрачное шифрование информации;
- трансляцию внутренних сетевых адресов для исходящих потоков сообщений.

Сначала протокол SOCKS разрабатывался только для перенаправления запросов к серверам со стороны клиентских приложений, а также возврата этим приложениям полученных ответов. Перенаправление запросов и ответов между клиент/серверными приложениями уже позволяет реализовать функцию трансляции сетевых IP-адресов NAT (Network Address Translation). Замена у исходящих пакетов внутренних IP-адресов отправителей одним IP-адресом шлюза позволяет скрыть топологию внутренней сети от внешних пользователей и тем самым усложнить задачу несанкционированного доступа. Трансляция сетевых адресов помимо повышения безопасности позволяет расширить внутреннее адресное пространство сети за счет возможности поддержки собственной системы адресации.

На основе протокола SOCKS могут быть реализованы и другие функции посредничества по защите сетевого взаимодействия. Например, протокол SOCKS может применяться для контроля над направлениями информационных потоков и разграничения доступа в зависимости от атрибутов пользователей и информации. Эффективность использования протокола SOCKS для выполнения функций посредни-

чества обеспечивается его ориентацией на сеансовый уровень модели OSI. По сравнению с посредниками прикладного уровня на сеансовом уровне достигаются более высокое быстродействие и независимость от высокоуровневых протоколов (HTTP, FTP, POP3, SMTP и др.). Кроме того, протокол SOCKS не привязан к протоколу IP и не зависит от операционных систем. Например, для обмена информацией между клиентскими приложениями и посредником может использоваться протокол IPX.

Благодаря протоколу SOCKS межсетевые экраны и виртуальные частные сети могут организовать безопасное взаимодействие и обмен информацией между разными сетями. Протокол SOCKS позволяет реализовать безопасное управление этими системами на основе унифицированной стратегии. Следует отметить, что на основе протокола SOCKS могут создаваться защищенные туннели для каждого приложения и сеанса в отдельности.

Согласно спецификации протокола SOCKS различают *SOCKS-сервер*, который целесообразно устанавливать на шлюз (межсетевой экран) сети, и *SOCKS-клиент*, который устанавливают на каждый пользовательский компьютер. SOCKS-сервер обеспечивает взаимодействие с любым прикладным сервером от имени соответствующего этому серверу прикладного клиента. SOCKS-клиент предназначен для перехвата всех запросов к прикладному серверу со стороны клиента и передачи их SOCKS-серверу. Следует отметить, что SOCKS-клиенты, выполняющие перехват запросов клиентских приложений и взаимодействие с SOCKS-сервером, могут быть встроены в универсальные клиентские программы. SOCKS-серверу известно о трафике на уровне сеанса (сокета), поэтому он может осуществлять тщательный контроль и, в частности, блокировать работу конкретных приложений пользователей, если они не имеют необходимых полномочий на информационный обмен.

Протокол SOCKS v5 одобрен организацией IETF (Internet Engineering Task Force) в качестве стандарта Интернета и включен в RFC 1928 (Request for Comments) [11].

Общая схема установления соединения по протоколу SOCKS версии 5 может быть описана следующим образом:

- запрос прикладного клиента, желающего установить соединение с каким-либо прикладным сервером в сети, перехватывает установленный на этом же компьютере SOCKS-клиент;
- соединившись с SOCKS-сервером, SOCKS-клиент сообщает ему идентификаторы всех методов аутентификации, которые он поддерживает;
- SOCKS-сервер решает, каким методом аутентификации воспользоваться (если SOCKS-сервер не поддерживает ни один из методов аутентификации, предложенных SOCKS-клиентом, соединение разрывается);
- при поддержке каких-либо предложенных методов аутентификации SOCKS-сервер в соответствии с выбранным методом аутентифицирует пользователя, от имени которого выступает SOCKS-кли-

ент; в случае безуспешной аутентификации SOCKS-сервер разрывает соединение;

- после успешной аутентификации SOCKS-клиент передает SOCKS-серверу DNS-имя или IP-адрес запрашиваемого прикладного сервера в сети, и далее SOCKS-сервер на основе имеющихся правил разграничения доступа принимает решение об установлении соединения с этим прикладным сервером;
- в случае установления соединения прикладной клиент и прикладной сервер взаимодействуют друг с другом по цепочке соединений, в которой SOCKS-сервер ретранслирует данные, а также может выполнять функции посредничества по защите сетевого взаимодействия: например, если в ходе аутентификации SOCKS-клиент и SOCKS-сервер обменялись сеансовым ключом, то весь трафик между ними может шифроваться.

Аутентификация пользователя, выполняемая SOCKS-сервером, может основываться на цифровых сертификатах в формате X.509 или паролях. Для шифрования трафика между SOCKS-клиентом и SOCKS-сервером могут быть использованы протоколы, ориентированные на сеансовый или более низкие уровни модели OSI. Кроме аутентификации пользователей, трансляции IP-адресов и криптозащиты трафика SOCKS-сервер может выполнять также такие функции, как:

- разграничение доступа к ресурсам внутренней сети;
- разграничение доступа к ресурсам внешней сети;
- фильтрация потока сообщений, например динамический поиск вирусов;
- регистрация событий и реагирование на задаваемые события;
- кэширование данных, запрашиваемых из внешней сети.

Протокол SOCKS осуществляет встроенную поддержку популярных веб-браузеров Netscape Navigator и Netscape Communicator компании Netscape, а также Internet Explorer компании «Майкрософт».

Специальные программы, называемые соксификаторами, дополняют клиентские приложения поддержкой протокола SOCKS. К таким программам относится, например, NEC SocksCap и др. При установке соксификатор внедряется между пользовательскими приложениями и стеком коммуникационных протоколов. Далее в процессе работы он перехватывает коммуникационные вызовы, формируемые приложениями, и перенаправляет их в случае надобности на SOCKS-сервер. При отсутствии нарушений установленных правил безопасности работа SOCKS-клиента совершенно прозрачна для клиентских приложений и пользователей.

Таким образом, для формирования защищенных виртуальных сетей по протоколу SOCKS в точке сопряжения каждой локальной сети с Интернетом на компьютере-шлюзе устанавливается SOCKS-сервер, а на рабочих станциях в локальных сетях и на компьютерах удаленных пользователей — SOCKS-клиенты. По существу, SOCKS-сервер можно рассматривать как межсетевой экран, поддерживающий протокол SOCKS (рис. 9.19).

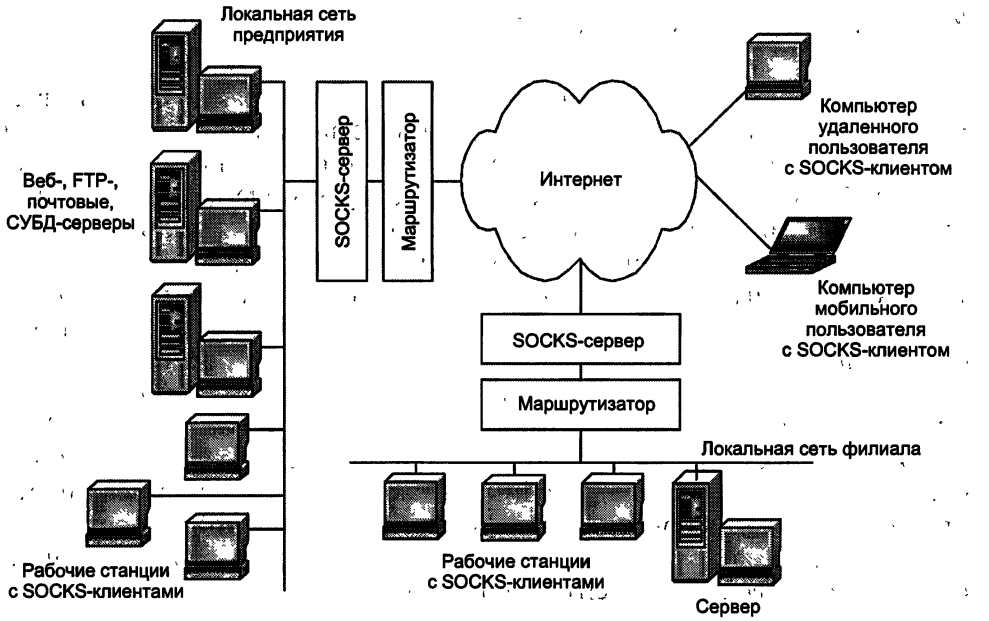


Рис. 9.19. Схема взаимодействия по протоколу SOCKS

Удаленные пользователи могут подключаться к Интернету любым способом — по коммутируемой или выделенной линии. При попытке пользователя защищенной виртуальной сети установить соединение с каким-либо прикладным сервером SOCKS-клиент начинает взаимодействовать с SOCKS-сервером. По завершении первого этапа взаимодействия пользователь будет аутентифицирован, а проверка правил доступа покажет, имеет ли он право соединиться с конкретным серверным приложением, функционирующим на компьютере с указанным адресом. Дальнейшее взаимодействие может происходить по криптографически защищенному каналу [41].

Помимо защиты локальной сети от несанкционированного доступа на SOCKS-сервер может возлагаться контроль доступа пользователей этой локальной сети к открытым ресурсам Интернета (Telnet, WWW, SMTP, POP и др.). Доступ является полностью авторизованным, так как идентифицируются и аутентифицируются конкретные пользователи, а не компьютеры, с которых они входят в сеть. Правила доступа могут запрещать или разрешать соединения с конкретными ресурсами Интернета в зависимости от полномочий конкретного сотрудника. Действие правил доступа может зависеть и от других параметров, например от метода аутентификации или времени суток.

В дополнение к функциям разграничения доступа может выполняться регистрация событий и реагирование на задаваемые события. Для достижения более высокой степени безопасности сетевого взаимодействия серверы локальной сети, к которым разрешен доступ со стороны Интернета, должны быть выделены в отдельный подсоединяемый к SOCKS-серверу сегмент, образующий защищаемую открытую подсеть.

9.4. Защита беспроводных сетей

Беспроводные сети начинают использоваться практически во всем мире. Это обусловлено их удобством, гибкостью и сравнительно невысокой стоимостью. Беспроводные технологии должны удовлетворять ряду требований к качеству, скорости, радиусу приема и защищенности, причем защищенность часто является самым важным фактором.

Сложность обеспечения безопасности беспроводной сети очевидна. Если в проводных сетях злоумышленник должен сначала получить физический доступ к кабельной системе или оконечным устройствам, то в беспроводных сетях это условие отпадает само собой: поскольку данные передаются «по воздуху», для получения доступа достаточно обычного приемника, установленного в радиусе действия сети (см. раздел 2.2).

Однако, несмотря на различия в реализации, подход к безопасности беспроводных сетей и их проводных аналогов идентичен: здесь присутствуют такие же требования к обеспечению конфиденциальности и целостности передаваемых данных и, конечно же, к проверке подлинности как беспроводных клиентов, так и точек доступа.

Общие сведения

Как и все стандарты IEEE 802, стандарт 802.11 работает на нижних двух уровнях модели ISO/OSI — физическом и канальном. Любое сетевое приложение, сетевая операционная система или протокол (например, TCP/IP) будут так же хорошо работать в сети 802.11, как и в сети Ethernet.

Основная архитектура, особенности и службы определяются в базовом стандарте 802.11 (см. главу 16). Стандарт 802.11 определяет два режима работы беспроводной сети — режим клиент/сервер (или режим инфраструктуры) и режим точка—точка (Ad-hoc).

В режиме клиент/сервер беспроводная сеть состоит как минимум из одной точки доступа AP (Access Point), подключенной к проводной сети, и некоторого набора беспроводных оконечных станций. Такая конфигурация носит название базового набора служб BSS (Basic Service Set). Два или более BSS, образующих единую подсеть, формируют расширенный набор служб ESS (Extended Service Set). Так как большинству беспроводных станций требуется получать доступ к файловым серверам, принтерам, Интернету, доступным в проводной локальной сети, они будут работать в режиме клиент/сервер.

Режим точка—точка (Ad-hoc) — это простая сеть, в которой связь между многочисленными станциями устанавливается напрямую, без использования специальной точки доступа. Такой режим полезен в том случае, если инфраструктура беспроводной сети не сформирована (например, отель, выставочный зал, аэропорт).

На физическом уровне стандарта 802.11 определены два широкополосных радиочастотных метода передачи и один — в инфракрасном

диапазоне. Радиочастотные методы работают в ISM диапазоне 2,4 ГГц и обычно используют полосу 83 МГц от 2,400 до 2,483 ГГц. Технологии широкополосного сигнала, используемые в радиочастотных методах, увеличивают надежность, пропускную способность, позволяют многим не связанным друг с другом устройствам разделять одну полосу частот с минимальными помехами друг для друга.

Основное дополнение, внесенное 802.11b в основной стандарт, — это поддержка двух новых скоростей передачи данных — 5,5 и 11 Мбит/с. Для достижения этих скоростей был выбран метод прямой последовательности DSSS (Direct Sequence Spread Spectrum).

Канальный (Data Link) уровень 802.11 состоит из двух подуровней: управления логической связью LLC (Logical Link Control) и управления доступом к носителю MAC (Media Access Control).

Обеспечение безопасности беспроводных сетей

Система защиты беспроводных сетей WLAN, основанная на протоколе WEP (Wired Equivalent Privacy) первоначального стандарта 802.11 страдает существенными недостатками. К счастью, появились более эффективные технологии обеспечения информационной безопасности WLAN, которые описаны в стандарте WPA (Wi-Fi Protected Access) организации Wi-Fi Alliance и стандарте 802.11i института IEEE и призваны устранить недостатки стандарта 802.11. Поскольку процесс разработки стандарта 802.11i слишком затянулся, организация Wi-Fi Alliance была вынуждена предложить в 2002 г. собственную технологию обеспечения информационной безопасности WLAN — стандарт WPA.

Стандарт WPA весьма привлекателен тем, что относительно прост в реализации и позволяет защитить ныне действующие WLAN. Стандарты WPA и 802.11i совместимы друг с другом, поэтому использование поддерживающих WPA продуктов можно считать начальным этапом перехода к системе защиты на базе стандарта 802.11i.

Между технологиями 802.11i и WPA много общего. Так, в них определена идентичная архитектура системы безопасности с улучшенными механизмами аутентификации пользователей и протоколами распространения и обновления ключей. Но есть и существенные различия. Например, технология WPA базируется на протоколе динамических ключей TKIP (Temporal Key Integrity Protocol), поддержку которого в большинстве устройств WLAN можно реализовать путем обновления их ПО, а в более функциональной концепции 802.11i предусмотрено использование нового стандарта шифрования AES (Advanced Encryption Standard), с которым совместимо лишь новейшее оборудование для WLAN.

В стандарте WPA предусмотрено использование защитных протоколов 802.1x, EAP, TKIP и RADIUS.

Механизм аутентификации пользователей основан на протоколе контроля доступа 802.1x (разработан для проводных сетей) и протоколе расширенной аутентификации EAP (Extensible Authentication Protocol).

Последний позволяет сетевому администратору задействовать алгоритмы аутентификации пользователей посредством сервера RADIUS (см. главу 12).

Функции обеспечения конфиденциальности и целостности данных базируются на протоколе TKIP, который, в отличие от протокола WEP, использует более эффективный механизм управления ключами, но тот же самый алгоритм RC4 для шифрования данных. Согласно протоколу TKIP сетевые устройства работают с 48-битным вектором инициализации (в отличие от 24-битного вектора инициализации протокола WEP) и реализуют правила изменения последовательности его битов, что исключает повторное использование ключей и осуществление повторных атак.

В протоколе TKIP предусмотрены генерация нового ключа для каждого передаваемого пакета и улучшенный контроль целостности сообщений с помощью криптографической контрольной суммы MIC (Message Integrity Code), препятствующей хакеру изменять содержимое передаваемых пакетов.

Система сетевой безопасности стандарта WPA работает в двух режимах: PSK (Pre-Shared Key) и Enterprise (корпоративный). Для развертывания системы, работающей в режиме PSK, необходим разделяемый пароль. Такую систему несложно устанавливать, но она защищает WLAN не столь надежно, как это делает система, функционирующая в режиме Enterprise с иерархией динамических ключей. Хотя протокол TKIP работает с тем же самым блочным шифром RC4, который предусмотрен спецификацией протокола WEP, технология WPA защищает данные надежнее последнего.

Чтобы точки доступа WLAN стали совместимыми со стандартом WPA, достаточно модернизировать их ПО. Для перевода же сетевой инфраструктуры на стандарт 802.11i потребуется новое оборудование, поддерживающее алгоритм шифрования AES. Дело в том, что AES-шифрование создает большую нагрузку на центральный процессор беспроводного клиентского устройства.

Чтобы корпоративные точки доступа работали в системе сетевой безопасности стандарта WPA или 802.11i, они должны поддерживать аутентификацию пользователей по протоколу RADIUS и реализовывать предусмотренный стандартом метод шифрования — TKIP или AES, — что потребует модернизации их ПО. И еще одно требование — быстро осуществлять повторную аутентификацию пользователей после разрыва соединения с сетью. Это особенно важно для нормального функционирования приложений, работающих в реальном масштабе времени.

Если сервер RADIUS, применяемый для контроля доступа пользователей проводной сети, поддерживает нужные методы аутентификации EAP, то его можно задействовать и для аутентификации пользователей WLAN. В противном случае следует установить сервер WLAN RADIUS. Этот сервер работает следующим образом: сначала он проверяет аутентифицирующую информацию пользователя (на соответствие содержимому своей базы данных об их идентификаторах и паролях) или его цифровой сертификат, а затем активизирует динамическую ге-

нерацию ключей шифрования точкой доступа и клиентской системой для каждого сеанса связи.

Для работы технологии WPA требуется механизм EAP-TLS (Transport Layer Security), тогда как в стандарте IEEE 802.11i применение конкретных методов аутентификации EAP не оговаривается. Выбор метода аутентификации EAP определяется спецификой работы клиентских приложений и архитектурой сети. Чтобы ноутбуки и карманные ПК работали в системе сетевой безопасности стандарта WPA или 802.11i, они должны быть оснащены клиентскими программами, поддерживающими стандарт 802.1x.

Самым простым с точки зрения развертывания вариантом системы сетевой безопасности стандарта WPA является система, работающая в режиме PSK. Она предназначена для небольших и домашних офисов и не нуждается в сервере RADIUS, а для шифрования пакетов и расчета криптографической контрольной суммы MIC в ней используется пароль PSK. Обеспечиваемый ею уровень информационной безопасности сети вполне достаточен для большинства вышеуказанных офисов. С целью повышения эффективности защиты данных следует применять пароли, содержащие не менее 20 символов.

Предприятиям целесообразно внедрять у себя системы сетевой безопасности стандарта WPA с серверами RADIUS. Большинство компаний предпочитают именно такие системы, поскольку работающие в режиме PSK решения сложнее администрировать и они более уязвимы для хакерских атак.

До тех пор пока средства стандарта 802.11i не станут доступными на рынке, WPA будет оставаться самым подходящим стандартом для защиты WLAN.

Стандарты WPA и 802.11i в достаточной степени надежны и обеспечивают высокий уровень защищенности беспроводных сетей. Тем не менее одного протокола защиты недостаточно — следует также уделить внимание правильному построению и настройке сети.

Физическая защита. При развертывании Wi-Fi-сети необходимо физически ограничить доступ к беспроводным точкам.

Правильная настройка. Парадокс современных беспроводных сетей заключается в том, что пользователи не всегда включают и используют встроенные механизмы аутентификации и шифрования.

Защита пользовательских устройств. Не следует полностью полагаться на встроенные механизмы защиты сети. Наиболее оптимальным является метод эшелонированной обороны, первой линией которой станут средства защиты, установленные на стационарном ПК, ноутбуке или КПК.

Традиционные меры. Эффективная работа компьютера в сети немыслима без классических мер защиты. Имеется в виду своевременная установка обновлений, использование защитных механизмов, встроенных в операционную систему и приложения, а также антивирусов. Однако этих мер на сегодня недостаточно, так как они ориентированы на защиту от уже известных угроз.

Мониторинг сети. Слабое звено в корпоративной сети — самовольно установленные точки доступа. Актуальной является задача локализации несанкционированных точек доступа. Специальные средства локализации точек доступа позволяют графически отображать место расположения «чужого» терминала на карте этажа или здания. Если классические методы не спасают от вторжения, на помощь приходят системы обнаружения атак.

VPN-агенты. Многие точки доступа работают в открытом режиме, поэтому необходимо использовать методы сокрытия передаваемых данных. На защищаемом компьютере должен быть установлен VPN-клиент, который возьмет на себя решение этой задачи. Практически все современные ОС (например, Windows XP) содержат в своем составе такие программные компоненты.

Вопросы для самоконтроля

1. Каковы назначение и особенности функционирования протокола PPTP?
2. Опишите архитектуру протокола L2TP.
3. Каковы возможности и особенности функционирования протокола L2TP?
4. Как осуществляется формирование защищенного виртуального канала по протоколу L2TP?
5. Каковы назначение и основные компоненты стека протоколов IPSec?
6. Опишите архитектуру средств безопасности IPSec.
7. Как осуществляется защита передаваемых данных с помощью протоколов AH и ESP в IPSec?
8. Опишите алгоритмы аутентификации и шифрования, используемые в IPSec.
9. Укажите назначение и особенности функционирования протокола IKE в IPSec.
10. Какие функции безопасности предоставляет протокол SSL? Каковы достоинства и недостатки протокола SSL?
11. Укажите назначение и особенности функционирования протокола SOCKS.
12. Какие стандарты и протоколы используют для обеспечения безопасности беспроводных сетей?

Глава 10
МЕЖСЕТЕВОЕ ЭКРАНИРОВАНИЕ

Межсетевое экранирование является одним из основных элементов эшелонированной обороны корпоративной сети.

Межсетевой экран (МЭ) — это специализированный комплекс межсетевой защиты, называемый также системой *firewall* или брандмауэром. Межсетевой экран позволяет разделить общую сеть на две части или более и реализовать набор правил, определяющих условия прохождения пакетов с данными через границу из одной части общей сети в другую. Как правило, эта граница проводится между корпоративной (локальной) сетью предприятия и глобальной сетью Интернет.

Обычно межсетевые экраны защищают внутреннюю сеть предприятия от вторжений из глобальной сети Интернет, хотя они могут использоваться и для защиты от нападений из корпоративной интрасети, к которой подключена локальная сеть предприятия. Технология межсетевых экранов стала одной из самых первых технологий защиты корпоративных сетей от внешних угроз.

Для большинства организаций установка межсетевого экрана является необходимым условием обеспечения безопасности внутренней сети.

10.1. Функции межсетевых экранов

Для противодействия несанкционированному межсетевому доступу межсетевой экран (МЭ) должен располагаться между защищаемой сетью организации, являющейся внутренней, и потенциально враждебной внешней сетью (рис. 10.1). При этом все взаимодействия между этими сетями должны осуществляться только через межсетевой экран. Организационно межсетевой экран входит в состав защищаемой сети.

Межсетевой экран, защищающий сразу множество узлов внутренней сети, призван решить две основные задачи:

- ограничение доступа внешних (по отношению к защищаемой сети) пользователей к внутренним ресурсам корпоративной сети. К таким пользователям могут быть отнесены партнеры, удаленные пользователи, хакеры и даже сотрудники самой компании, пытающиеся получить доступ к серверам баз данных, защищаемых межсетевым экраном;
- разграничение доступа пользователей защищаемой сети к внешним ресурсам. Решение этой задачи позволяет, например, регули-

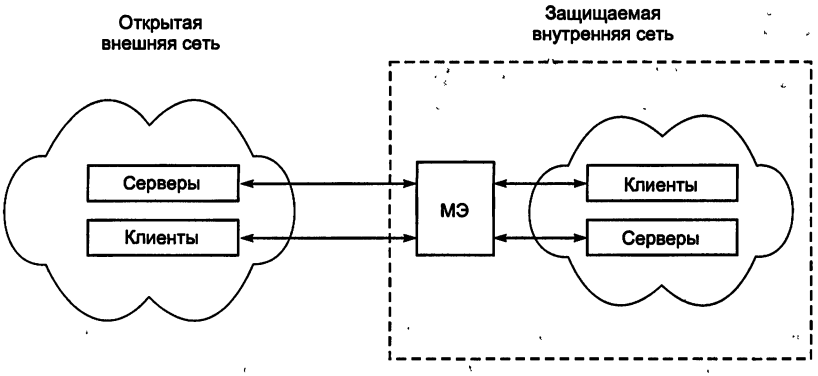


Рис. 10.1. Схема подключения межсетевого экрана

ровать доступ к серверам, не требуемым для выполнения служебных обязанностей.

До сих пор не существует единой общепризнанной классификации межсетевых экранов. МЭ можно классифицировать по следующим основным признакам [27].

По функционированию на уровнях модели OSI:

- пакетный фильтр (экранирующий маршрутизатор — Screening Router);
- шлюз сеансового уровня (экранирующий транспорт);
- прикладной шлюз (Application Gateway);
- шлюз экспертного уровня (Stateful Inspection Firewall).

По используемой технологии:

- контроль состояния протокола (Stateful Inspection);
- на основе модулей посредников (прокси).

По исполнению:

- аппаратно-программный;
- программный.

По схеме подключения:

- схема единой защиты сети;
- схема с защищаемым закрытым и не защищаемым открытым сегментами сети;
- схема с раздельной защитой закрытого и открытого сегментов сети.

10.1.1. Фильтрация трафика

Фильтрация информационных потоков состоит в их выборочном пропускании через экран, возможно, с выполнением некоторых преобразований [7, 27]. Фильтрация осуществляется на основе набора предварительно загруженных в межсетевой экран правил, соответствующих принятой политике безопасности. Поэтому межсетевой экран удобно представлять как последовательность фильтров, обрабатывающих информационный поток (рис. 10.2).

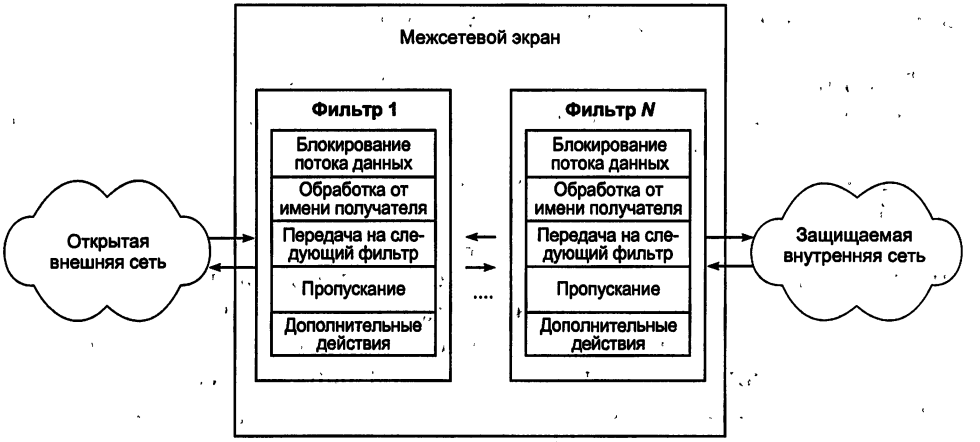


Рис. 10.2. Структура межсетевого экрана

Каждый из фильтров предназначен для интерпретации отдельных правил фильтрации путем выполнения следующих действий:

1. Анализ информации по заданным в интерпретируемых правилах критериям, например по адресам получателя и отправителя или по типу приложения, для которого эта информация предназначена.

2. Принятие на основе интерпретируемых правил одного из следующих решений:

- не пропустить данные;
- обработать данные от имени получателя и возвратить результат отправителю;
- передать данные на следующий фильтр для продолжения анализа;
- пропустить данные, игнорируя следующие фильтры.

Правила фильтрации могут задавать и дополнительные действия, которые относятся к функциям посредничества, например преобразование данных, регистрацию событий и др. Соответственно, правила фильтрации определяют перечень условий, по которым осуществляется:

- разрешение или запрещение дальнейшей передачи данных;
- выполнение дополнительных защитных функций.

В качестве критериев анализа информационного потока могут использоваться следующие параметры:

- служебные поля пакетов сообщений, содержащие сетевые адреса, идентификаторы, адреса интерфейсов, номера портов и другие значимые данные;
- непосредственное содержимое пакетов сообщений, проверяемое, например, на наличие компьютерных вирусов;
- внешние характеристики потока информации, например временные, частотные характеристики, объем данных и т. д.

Используемые критерии анализа зависят от уровней модели OSI, на которых осуществляется фильтрация. В общем случае чем выше уровень модели OSI, на котором МЭ фильтрует пакеты, тем выше и обеспечиваемый им уровень защиты.

10.1.2. Выполнение функций посредничества

Функции посредничества МЭ выполняет с помощью специальных программ, называемых *программами-посредниками* или *экранирующими агентами*. Данные программы являются резидентными и запрещают непосредственную передачу пакетов сообщений между внешней и внутренней сетью.

При необходимости доступа из внутренней сети во внешнюю сеть или наоборот вначале должно быть установлено логическое соединение с программой-посредником, функционирующей на компьютере МЭ. Программа-посредник проверяет допустимость запрошенного межсетевого взаимодействия и при его разрешении сама устанавливает отдельное соединение с требуемым компьютером. Далее обмен информацией между компьютерами внутренней и внешней сети осуществляется через программного посредника, который может выполнять фильтрацию потока сообщений, а также осуществлять другие защитные функции.

Следует иметь в виду, что МЭ может выполнять функции фильтрации без применения программ-посредников, обеспечивая прозрачное взаимодействие между внутренней и внешней сетью. Вместе с тем программные посредники могут и не осуществлять фильтрацию потока сообщений.

В общем случае программы-посредники, блокируя прозрачную передачу потока сообщений, могут выполнять следующие функции:

- проверку подлинности передаваемых данных;
- фильтрацию и преобразование потока сообщений, например динамический поиск вирусов и прозрачное шифрование информации;
- разграничение доступа к ресурсам внутренней сети;
- разграничение доступа к ресурсам внешней сети;
- кэширование данных, запрашиваемых из внешней сети.
- идентификацию и аутентификацию пользователей;
- трансляцию внутренних сетевых адресов для исходящих пакетов сообщений;
- регистрацию событий, реагирование на задаваемые события, а также анализ зарегистрированной информации и генерацию отчетов [7, 27].

Программы-посредники могут осуществлять *проверку подлинности получаемых и передаваемых данных*. Это актуально для аутентификации не только электронных сообщений, но и мигрирующих программ (Java, ActiveX Controls), по отношению к которым может быть выполнен подлог. Проверка подлинности сообщений и программ заключается в контроле их цифровых подписей.

Программы-посредники могут выполнять *разграничение доступа к ресурсам внутренней или внешней сети*, используя результаты идентификации и аутентификации пользователей при их обращении к межсетевому экрану.

Способы *разграничения доступа к ресурсам внутренней сети* практически не отличаются от способов разграничения, поддерживаемых на уровне операционной системы.

При *разграничении доступа к ресурсам внешней сети* чаще всего используется один из следующих подходов:

- разрешение доступа только по заданным адресам во внешней сети;
- фильтрация запросов на основе обновляемых списков недопустимых адресов и блокировка поиска информационных ресурсов по нежелательным ключевым словам;
- накопление и обновление администратором санкционированных информационных ресурсов внешней сети в дисковой памяти МЭ и полный запрет доступа во внешнюю сеть.

С помощью специальных посредников поддерживается также *кэширование данных*, запрашиваемых из внешней сети. При доступе пользователей внутренней сети к информационным ресурсам внешней сети вся информация накапливается на пространстве жесткого диска МЭ, называемого в этом случае прокси-сервером. Поэтому если при очередном запросе нужная информация окажется на прокси-сервере, то посредник предоставляет ее без обращения к внешней сети, что существенно ускоряет доступ. Администратору следует позаботиться только о периодическом обновлении содержимого прокси-сервера.

Функция кэширования успешно может использоваться для ограничения доступа к информационным ресурсам внешней сети. В этом случае все санкционированные информационные ресурсы внешней сети накапливаются и обновляются администратором на прокси-сервере. Пользователям внутренней сети разрешается доступ только к информационным ресурсам прокси-сервера, а непосредственный доступ к ресурсам внешней сети запрещается.

Фильтрация и преобразование потока сообщений выполняется посредником на основе заданного набора правил. Здесь следует различать два вида программ-посредников:

- экранирующие агенты, ориентированные на анализ потока сообщений для определенных видов сервиса, например FTP, HTTP, Telnet;
- универсальные экранирующие агенты, обрабатывающие весь поток сообщений, например агенты, ориентированные на поиск и обезвреживание компьютерных вирусов или прозрачное шифрование данных.

Программный посредник анализирует поступающие к нему пакеты данных, и если какой-либо объект не соответствует заданным критериям, то посредник либо блокирует его дальнейшее продвижение, либо выполняет соответствующие преобразования, например обезвреживание обнаруженных компьютерных вирусов. При анализе содержимого пакетов важно, чтобы экранирующий агент мог автоматически распаковывать проходящие файловые архивы.

МЭ с посредниками позволяют также организовывать защищенные виртуальные сети VPN, например безопасно объединить несколько локальных сетей, подключенных к Интернету, в одну виртуальную сеть.

Помимо выполнения фильтрации трафика и функций посредничества, современные межсетевые экраны позволяют реализовать ряд других, не менее важных функций, без которых обеспечение защиты периметра внутренней сети было бы неполным [7]. Рассмотрим дополнительные возможности современных межсетевых экранов.

10.1.3. Дополнительные возможности МЭ

Рассмотрим реализацию межсетевыми экранами таких функций, как идентификация и аутентификация пользователей, трансляция внутренних сетевых адресов для исходящих пакетов сообщений, регистрация событий, реагирование на задаваемые события, анализ зарегистрированной информации и генерация отчетов.

Идентификация и аутентификация пользователей. Кроме разрешения или запрещения допуска различных приложений в сеть, межсетевые экраны могут также выполнять аналогичные действия и для пользователей, которые желают получить доступ к внешним или внутренним ресурсам, разделяемым межсетевым экраном.

Прежде чем пользователю будет предоставлено право использовать какой-либо сервис, необходимо убедиться, что пользователь действительно тот, за кого себя выдает. Идентификация и аутентификация пользователей являются важными компонентами концепции межсетевых экранов. Авторизация пользователя обычно рассматривается в контексте аутентификации — как только пользователь аутентифицирован, для него определяются разрешенные ему сервисы.

Идентификация и аутентификация пользователя иногда осуществляются при предъявлении обычного идентификатора (имени) и пароля. Однако эта схема уязвима с точки зрения безопасности — пароль может быть перехвачен и использован другим лицом. Многие инциденты в сети Интернет произошли отчасти из-за уязвимости традиционных многоразовых паролей. Злоумышленники могут наблюдать за каналами в сети Интернет и перехватывать передающиеся в них открытым текстом пароли, поэтому такая схема аутентификации считается неэффективной. Пароль следует передавать через общедоступные коммуникации в зашифрованном виде (рис. 10.3). Это позволяет предотвратить получение несанкционированного доступа путем перехвата сетевых пакетов.

Более надежным методом аутентификации является использование одноразовых паролей. Широкое распространение получила технология аутентификации на основе одноразовых паролей SecurID, разработанная компанией Security Dynamics и реализованная в коммуникационных серверах ряда компаний, в частности в серверах компании Cisco Systems и др.

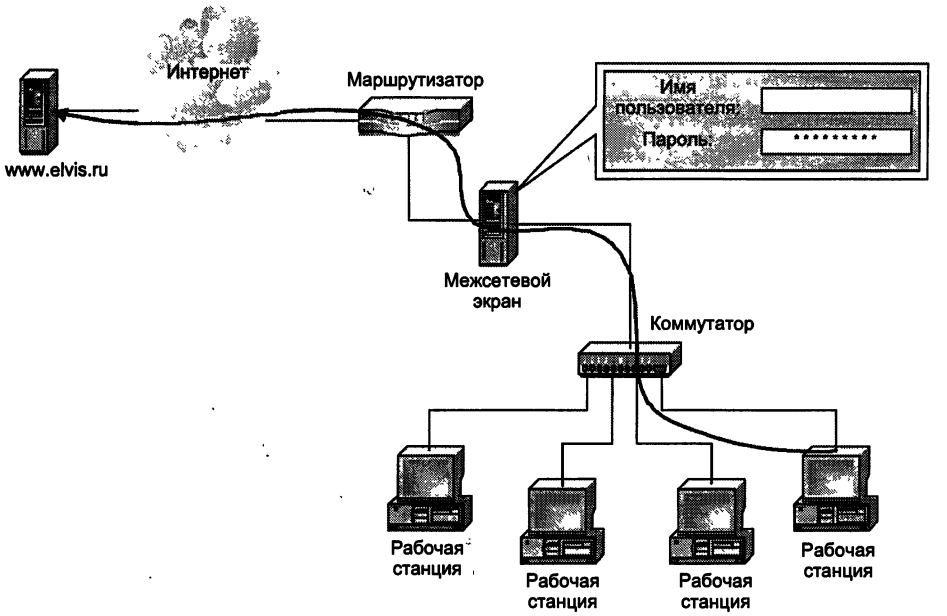


Рис. 10.3. Схема аутентификации пользователя по предъявляемому паролю

Удобно и надежно также применение цифровых сертификатов, выдаваемых доверенными органами, например центром распределения ключей. Большинство программ-посредников разрабатываются таким образом, чтобы пользователь аутентифицировался только в начале сеанса работы с межсетевым экраном. После этого от него не требуется дополнительная аутентификация в течение времени, определяемого администратором.

Так как межсетевые экраны могут централизовать управление доступом в сети, они являются подходящим местом для установки программ или устройств усиленной аутентификации. Хотя средства усиленной аутентификации могут использоваться на каждом хосте, более практично их размещение на межсетевом экране. При отсутствии межсетевого экрана, использующего меры усиленной аутентификации, неаутентифицированный трафик таких приложений, как TELNET или FTP, может напрямую проходить к внутренним системам в сети.

Ряд межсетевых экранов поддерживают Kerberos — один из распространенных методов аутентификации. Как правило, большинство коммерческих межсетевых экранов поддерживают несколько различных схем аутентификации, позволяя администратору сетевой безопасности сделать выбор наиболее приемлемой схемы для своих условий.

Трансляция сетевых адресов. Для реализации многих атак злоумышленнику необходимо знать адрес своей жертвы. Чтобы скрыть эти адреса, а также топологию всей сети, межсетевые экраны выполняют очень важную функцию — трансляцию внутренних сетевых адресов (Network Address Translation) — рис. 10.4.

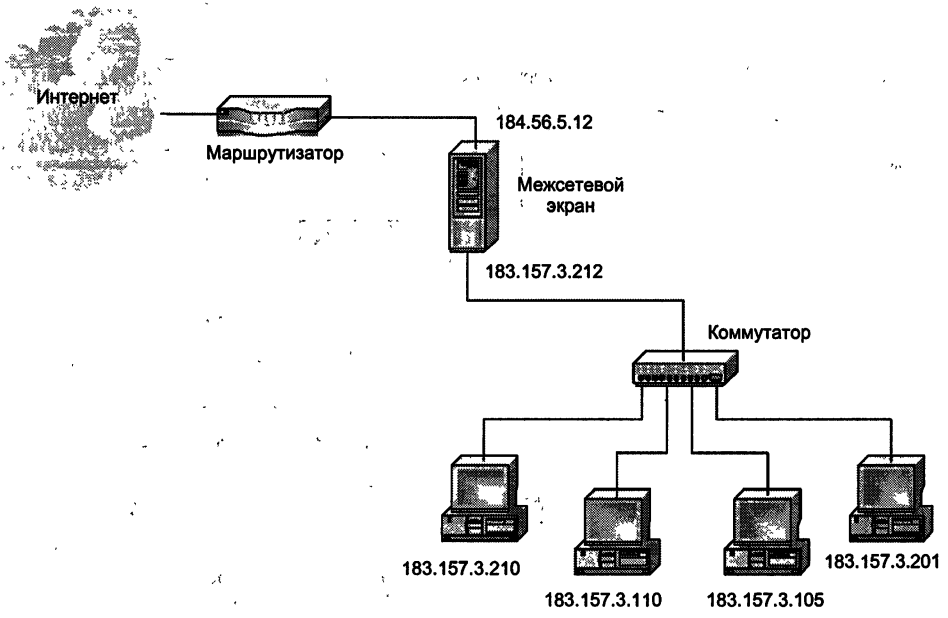


Рис. 10.4. Трансляция сетевых адресов

Данная функция реализуется по отношению ко всем пакетам, следующим из внутренней сети во внешнюю. Для этих пакетов выполняется автоматическое преобразование IP-адресов компьютеров-отправителей в один «надежный» IP-адрес.

Трансляция внутренних сетевых адресов может осуществляться двумя способами: динамически и статически. В первом случае адрес выделяется узлу в момент обращения к МЭ. После завершения соединения адрес освобождается и может быть использован любым другим узлом корпоративной сети. Во втором случае адрес узла всегда привязывается к одному адресу МЭ, из которого передаются все исходящие пакеты. IP-адрес МЭ становится единственным активным IP-адресом, который попадает во внешнюю сеть. В результате все исходящие из внутренней сети пакеты оказываются отправленными МЭ, что исключает прямой контакт между авторизованной внутренней сетью и являющейся потенциально опасной внешней сетью.

При таком подходе топология внутренней сети скрыта от внешних пользователей, что усложняет задачу несанкционированного доступа. Кроме повышения безопасности трансляция адресов позволяет иметь внутри сети собственную систему адресации, не согласованную с адресацией во внешней сети, например, в сети Интернет. Это эффективно решает проблему расширения адресного пространства внутренней сети и дефицита адресов внешней сети.

Администрирование, регистрация событий и генерация отчетов. Простота и удобство администрирования является одним из ключевых аспектов в создании эффективной и надежной системы защиты. Ошибки

при определении правил доступа могут образовать дыру, через которую может быть взломана система. Поэтому в большинстве межсетевых экранов реализованы сервисные утилиты, облегчающие ввод, удаление, просмотр набора правил. Наличие этих утилит позволяет также производить проверки на синтаксические или логические ошибки при вводе или редактировании правил. Как правило, эти утилиты позволяют просматривать информацию, сгруппированную по каким-либо критериям, — например, все, что относится к конкретному пользователю или сервису.

Важными функциями межсетевых экранов являются *регистрация событий*, *реагирование на задаваемые события*, а также *анализ зарегистрированной информации и составление отчетов*. Являясь критическим элементом системы защиты корпоративной сети, межсетевой экран имеет возможность регистрации всех действий, им фиксируемых. К таким действиям относятся не только пропуск или блокирование сетевых пакетов, но и изменение правил разграничения доступа администратором безопасности и другие действия. Такая регистрация позволяет обращаться к создаваемым журналам по мере необходимости — в случае возникновения инцидента безопасности или сбора доказательств для предоставления их в судебные инстанции либо для внутреннего расследования.

При правильно настроенной системе фиксации сигналов о подозрительных событиях (alarm) межсетевой экран может дать детальную информацию о том, были ли межсетевой экран или сеть атакованы либо зондированы. Собирать статистику использования сети и доказательства ее зондирования важно по ряду причин. Прежде всего, нужно знать наверняка, что межсетевой экран устойчив к зондированию и атакам, и определить, адекватны ли меры защиты межсетевого экрана. Кроме того, статистика использования сети важна в качестве исходных данных при проведении исследований и анализе риска для формулирования требований к сетевому оборудованию и программам.

Многие МЭ содержат мощную систему регистрации, сбора и анализа статистики. Учет может вестись по адресам клиента и сервера, идентификаторам пользователей, времени сеансов, времени соединений, количеству переданных/принятых данных, действиям администратора и пользователей. Системы учета позволяют произвести анализ статистики и предоставляют администраторам подробные отчеты. За счет использования специальных протоколов МЭ могут выполнить удаленное оповещение об определенных событиях в режиме реального времени.

В качестве обязательной реакции на обнаружение попыток выполнения несанкционированных действий должно быть определено уведомление администратора, т. е. выдача предупредительных сигналов. Любой МЭ, который не способен посылать предупредительные сигналы при обнаружении нападения, нельзя считать эффективным средством межсетевой защиты.

10.2. Особенности функционирования межсетевых экранов на различных уровнях модели OSI

МЭ поддерживают безопасность межсетевого взаимодействия на различных уровнях модели OSI. При этом функции защиты, выполняемые на разных уровнях эталонной модели, существенно отличаются друг от друга. Поэтому комплексный МЭ удобно представить в виде совокупности неделимых экранов, каждый из которых ориентирован на отдельный уровень модели OSI.

Чаще всего комплексный экран функционирует на сетевом, сеансовом и прикладном уровнях эталонной модели. Соответственно различают такие неделимые МЭ (рис. 10.5), как:

- экранирующий маршрутизатор;
- шлюз сеансового уровня;
- шлюз прикладного уровня (экранирующий шлюз) [7, 27].

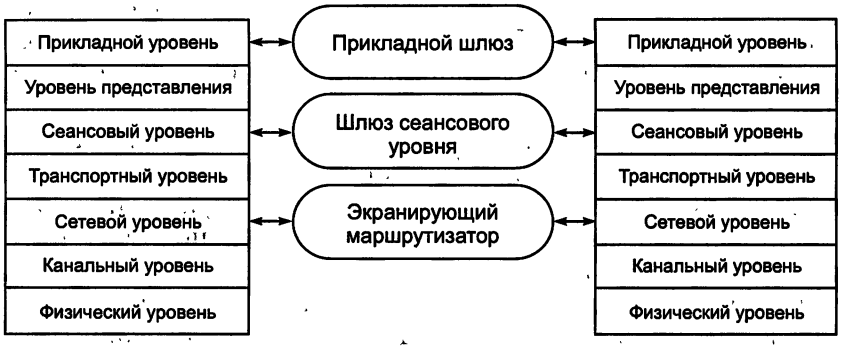


Рис. 10.5. Типы межсетевых экранов, функционирующих на отдельных уровнях модели OSI

Используемые в сетях протоколы (TCP/IP, SPX/IPX) не полностью соответствуют эталонной модели OSI, поэтому экраны перечисленных типов при выполнении своих функций могут охватывать и соседние уровни эталонной модели. Например, прикладной экран может осуществлять автоматическое зашифровывание сообщений при их передаче во внешнюю сеть, а также автоматическое расшифровывание криптографически закрытых принимаемых данных. В этом случае такой экран функционирует не только на прикладном уровне модели OSI, но и на уровне представления.

Шлюз сеансового уровня при своем функционировании охватывает транспортный и сетевой уровни модели OSI. Экранирующий маршрутизатор при анализе пакетов сообщений проверяет их заголовки не только сетевого, но и транспортного уровня.

Межсетевые экраны указанных типов имеют свои достоинства и недостатки. Многие из используемых МЭ являются либо прикладными шлюзами, либо экранирующими маршрутизаторами, не обеспечиваю-

щими полную безопасность межсетевого взаимодействия. Надежную же защиту обеспечивают только комплексные межсетевые экраны, каждый из которых объединяет экранирующий маршрутизатор, шлюз сеансового уровня, а также прикладной шлюз.

10.2.1. Экранирующий маршрутизатор

Экранирующий маршрутизатор (Screening Router), называемый также *пакетным фильтром (Packet Filter)*, предназначен для фильтрации пакетов сообщений и обеспечивает прозрачное взаимодействие между внутренней и внешней сетями. Он функционирует на сетевом уровне эталонной модели OSI, но для выполнения своих отдельных функций может охватывать и транспортный уровень эталонной модели.

Решение о том, пропустить или отбраковать данные, принимается для каждого пакета независимо на основе заданных правил фильтрации. Для принятия решения анализируются заголовки пакетов сетевого и транспортного уровней (рис. 10.6).

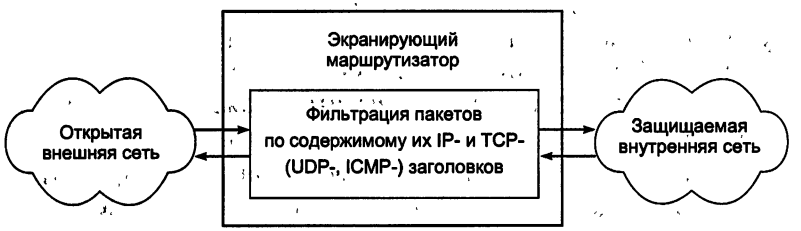


Рис. 10.6. Схема функционирования пакетного фильтра

В качестве анализируемых полей IP- и TCP- (UDP-) заголовков каждого пакета могут использоваться:

- адрес отправителя;
- адрес получателя;
- тип пакета;
- флаг фрагментации пакета;
- номер порта источника;
- номер порта получателя.

Первые четыре параметра относятся к IP-заголовку пакета, а следующие — к TCP- или UDP-заголовку. Адреса отправителя и получателя являются IP-адресами. Эти адреса заполняются при формировании пакета и остаются неизменными при передаче его по сети.

Поле типа пакета содержит код протокола ICMP, соответствующего сетевому уровню, либо код протокола транспортного уровня (TCP или UDP), к которому относится анализируемый IP-пакет.

Флаг фрагментации пакета определяет наличие или отсутствие фрагментации IP-пакетов. Если флаг фрагментации для анализируемого пакета установлен, то данный пакет является подпакетом фрагментированного IP-пакета.

Номера портов источника и получателя добавляются драйвером TCP или UDP к каждому отправляемому пакету сообщения и однозначно идентифицируют приложение-отправитель, а также приложение, для которого предназначен этот пакет. Для возможности фильтрации пакетов по номерам портов необходимо знание принятых в сети соглашений относительно выделения номеров портов протоколам высокого уровня.

При обработке каждого пакета экранирующий маршрутизатор последовательно просматривает заданную таблицу правил, пока не найдет правило, с которым согласуется полная ассоциация пакета. Здесь под ассоциацией понимается совокупность параметров, указанных в заголовках данного пакета. Если экранирующий маршрутизатор получил пакет, не соответствующий ни одному из табличных правил, он применяет правило, заданное по умолчанию. Из соображений безопасности это правило обычно указывает на необходимость отбраковки всех пакетов, не удовлетворяющих ни одному из других правил.

Пакетные фильтры могут быть реализованы как аппаратно, так и программно. В качестве пакетного фильтра могут быть использованы как обычный маршрутизатор, так и работающая на сервере программа, сконфигурированные таким образом, чтобы фильтровать входящие и исходящие пакеты. Современные маршрутизаторы, в частности компаний Cisco и Bay Networks, позволяют связывать с каждым портом несколько десятков правил и фильтровать пакеты как на входе, так и на выходе.

Обладая рядом положительных качеств, пакетные фильтры не лишены серьезных недостатков. Они не обеспечивают высокой степени безопасности, так как проверяют только заголовки пакетов и не поддерживают многие необходимые функции защиты, например аутентификацию конечных узлов, криптографическое закрытие пакетов сообщений, а также проверку их целостности и подлинности. Пакетные фильтры уязвимы для таких распространенных сетевых атак, как подмена исходных адресов и несанкционированное изменение содержимого пакетов сообщений. Однако такие достоинства пакетных фильтров, как простота реализации, высокая производительность, прозрачность для программных приложений и малая цена, обусловленная тем, что любой маршрутизатор в той или иной степени предоставляет возможность фильтрации пакетов, перевешивают указанные недостатки и обусловливают их повсеместное распространение и использование как обязательного элемента системы сетевой безопасности. Кроме того, они являются составной частью практически всех межсетевых экранов, использующих контроль состояния.

10.2.2. Шлюз сеансового уровня

Шлюз сеансового уровня, называемый еще *экранирующим транспортом*, предназначен для контроля виртуальных соединений и трансляции IP-адресов при взаимодействии с внешней сетью. Он функционирует на

сеансовом уровне модели OSI, охватывая в процессе своей работы также транспортный и сетевой уровни эталонной модели. Защитные функции шлюза сеансового уровня относятся к функциям посредничества.

Контроль виртуальных соединений заключается в контроле квитирования связи, а также передачи информации по установленным виртуальным каналам. При контроле квитирования связи шлюз сеансового уровня следит за установлением виртуального соединения между рабочей станцией внутренней сети и компьютером внешней сети, определяя, является ли запрашиваемый сеанс связи допустимым.

Такой контроль основывается на информации, содержащейся в заголовках пакетов сеансового уровня протокола TCP. Однако если пакетный фильтр при анализе TCP-заголовков проверяет только номера портов источника и получателя, то экранирующий транспорт анализирует другие поля, относящиеся к процессу квитирования связи.

Чтобы определить, является ли запрос на сеанс связи допустимым, шлюз сеансового уровня выполняет следующие действия. Когда рабочая станция (клиент) запрашивает связь с внешней сетью, шлюз принимает этот запрос, проверяя, удовлетворяет ли он базовым критериям фильтрации, например может ли сервер определить IP-адрес клиента и ассоциированное с ним имя. Затем, действуя от имени клиента, шлюз устанавливает соединение с компьютером внешней сети и следит за выполнением процедуры квитирования связи по протоколу TCP.

После того как шлюз определил, что рабочая станция внутренней сети и компьютер внешней сети являются авторизованными участниками сеанса TCP, и проверил допустимость данного сеанса, он устанавливает соединение.

Начиная с этого момента шлюз копирует и перенаправляет пакеты туда и обратно, контролируя передачу информации по установленному виртуальному каналу.

Для контроля виртуальных соединений в шлюзах сеансового уровня используются специальные программы, которые называют *канальными посредниками (Pipe Proxies)*. Эти посредники устанавливают между внутренней и внешней сетями виртуальные каналы, а затем контролируют передачу по этим каналам пакетов, генерируемых приложениями TCP/IP (рис. 10.7).

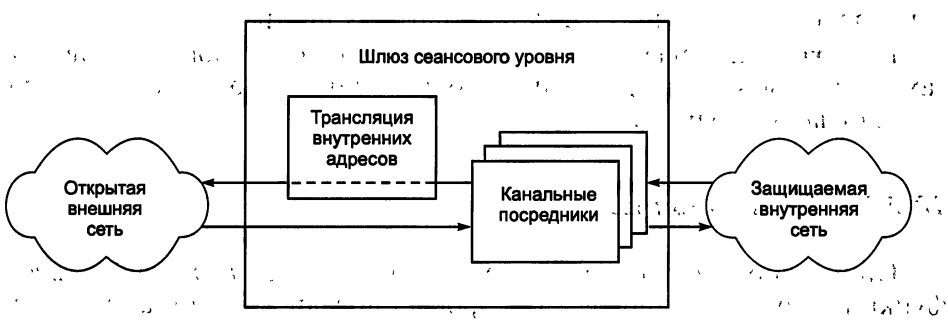


Рис. 10.7. Схема функционирования шлюза сеансового уровня

Канальные посредники ориентированы на конкретные службы TCP/IP. Поэтому шлюзы сеансового уровня могут использоваться для расширения возможностей шлюзов прикладного уровня, работа которых основывается на программах-посредниках конкретных приложений.

Шлюз сеансового уровня обеспечивает также трансляцию внутренних адресов сетевого уровня (IP-адресов) при взаимодействии с внешней сетью. Трансляция внутренних адресов выполняется по отношению ко всем пакетам, следующим из внутренней сети во внешнюю. Для этих пакетов IP-адреса компьютеров-отправителей внутренней сети автоматически преобразуются в один IP-адрес, ассоциируемый с экранирующим транспортом. В результате все пакеты, исходящие из внутренней сети, оказываются отправленными межсетевым экраном, что исключает прямой контакт между внутренней и внешней сетью. IP-адрес шлюза сеансового уровня становится единственным активным IP-адресом, который попадает во внешнюю сеть.

Трансляция адресов вызвана необходимостью усиления защиты путем сокрытия от внешних пользователей структуры защищаемой внутренней сети. При трансляции внутренних IP-адресов шлюз сеансового уровня экранирует, т. е. заслоняет, внутреннюю сеть от внешнего мира.

С другой стороны, трансляция адресов вызвана тем, что канальные посредники создают новое соединение каждый раз, когда они активизируются. Посредник принимает запрос от рабочей станции внутренней сети и затем инициирует новый запрос к компьютеру внешней сети. Поэтому компьютер внешней сети воспринимает запрос как исходящий от посредника, а не от действительного клиента.

С точки зрения реализации шлюз сеансового уровня представляет собой довольно простую и относительно надежную программу. Он дополняет экранирующий маршрутизатор функциями контроля виртуальных соединений и трансляции внутренних IP-адресов.

Недостатки у шлюза сеансового уровня те же, что и у экранирующего маршрутизатора, — не обеспечивается контроль и защита содержимого пакетов сообщений, не поддерживается аутентификация пользователей и конечных узлов, а также другие функции защиты локальной сети. У данной технологии есть еще один серьезный недостаток — невозможность проверки содержимого поля данных. В результате злоумышленнику предоставляется возможность передачи в защищаемую сеть троянских коней и других вредоносных программ.

На практике большинство шлюзов сеансового уровня не являются самостоятельными продуктами, а поставляются в комплекте со шлюзами прикладного уровня.

10.2.3. Прикладной шлюз

Прикладной шлюз, называемый также *экранирующим шлюзом*, функционирует на прикладном уровне модели OSI, охватывая также уровень представления, и обеспечивает надежную защиту межсетевых

взаимодействий [7, 27]. Защитные функции прикладного шлюза, как и шлюза сеансового уровня, относятся к функциям посредничества. Однако прикладной шлюз, в отличие от шлюза сеансового уровня, может выполнять существенно большее количество функций защиты, к которым относятся следующие:

- идентификация и аутентификация пользователей при попытке установления соединений через МЭ;
- проверка подлинности информации, передаваемой через шлюз;
- разграничение доступа к ресурсам внутренней и внешней сетей;
- фильтрация и преобразование потока сообщений, например динамический поиск вирусов и прозрачное шифрование информации;
- регистрация событий, реагирование на задаваемые события, а также анализ зарегистрированной информации и генерация отчетов;
- кэширование данных, запрашиваемых из внешней сети.

Поскольку функции прикладного шлюза относятся к функциям посредничества, этот шлюз представляет собой универсальный компьютер, на котором функционируют программные посредники (экранирующие агенты) — по одному для каждого обслуживаемого прикладного протокола (HTTP, FTP, SMTP, NNTP и др.). Программный посредник (Application Proxy) каждой службы TCP/IP ориентирован на обработку сообщений и выполнение функций защиты, относящихся именно к этой службе.

Прикладной шлюз перехватывает с помощью соответствующих экранирующих агентов входящие и исходящие пакеты, копирует и перенаправляет информацию, т. е. прикладной шлюз функционирует в качестве сервера-посредника, исключая прямые соединения между внутренней и внешней сетью (рис. 10.8).

Посредники, используемые прикладным шлюзом, имеют важные отличия от канальных посредников шлюзов сеансового уровня. Во-первых, посредники прикладного шлюза связаны с конкретными приложе-

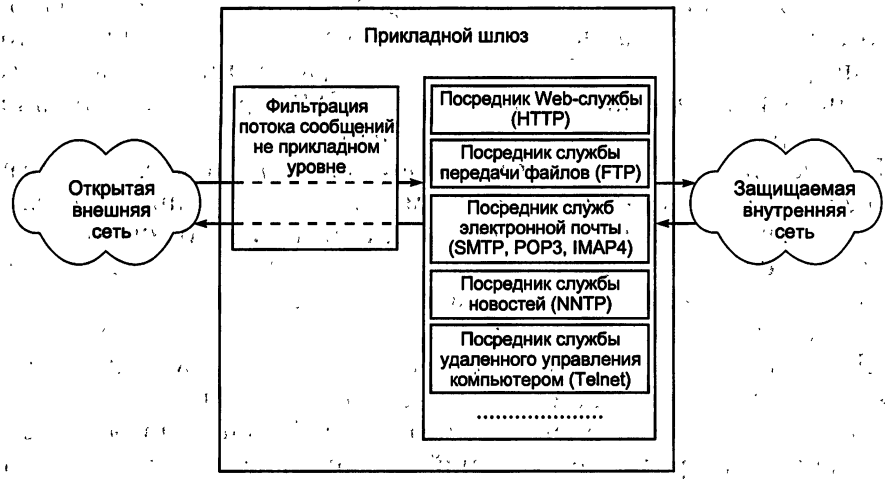


Рис. 10.8. Схема функционирования прикладного шлюза

ниями (программными серверами), во-вторых, они могут фильтровать поток сообщений на прикладном уровне модели OSI.

Прикладные шлюзы используют в качестве посредников специально разработанные для этой цели программные серверы конкретных служб TCP/IP — серверы HTTP, FTP, SMTP, NNTP и др. Эти программные серверы функционируют на МЭ в резидентном режиме и реализуют функции защиты, относящиеся к соответствующим службам TCP/IP. Трафик UDP обслуживается специальным транслятором содержимого UDP-пакетов.

Как и в случае шлюза сеансового уровня, для связи между рабочей станцией внутренней сети и компьютером внешней сети соответствующий посредник прикладного шлюза образует два соединения: от рабочей станции до МЭ и от МЭ до места назначения. Посредники прикладного шлюза пропускают только пакеты, сгенерированные теми приложениями, которые им поручено обслуживать. Например, программа-посредник службы HTTP может обрабатывать лишь трафик, генерируемый этой службой.

Если для какого-либо из приложений отсутствует свой посредник приложений, то прикладной шлюз не сможет обрабатывать трафик такого приложения и он будет блокирован. Например, если прикладной шлюз использует только программы-посредники HTTP, FTP и Telnet, то он будет обрабатывать лишь пакеты, относящиеся к этим службам, блокируя при этом пакеты всех остальных служб.

Фильтрация потоков сообщений реализуется прикладными шлюзами на прикладном уровне модели OSI. Соответственно, посредники прикладного шлюза, в отличие от канальных посредников, обеспечивают проверку содержимого обрабатываемых пакетов. Они могут фильтровать отдельные виды команд или информации в сообщениях протоколов прикладного уровня, которые им поручено обслуживать. Например, для службы FTP возможно динамическое обезвреживание компьютерных вирусов в копируемых из внешней сети файлах. Кроме того, посредник данной службы может быть сконфигурирован таким образом, чтобы предотвращать использование клиентами команды `PUT`, предназначенной для записи файлов на FTP-сервер. Такое ограничение уменьшает риск случайного повреждения хранящейся на FTP-сервере информации и снижает вероятность переполнения его ненужными данными.

При настройке прикладного шлюза и описании правил фильтрации сообщений используются такие параметры, как название сервиса; допустимый временной интервал его использования; ограничения на содержимое сообщений, связанных с данным сервисом; компьютеры, с которых можно пользоваться сервисом; идентификаторы пользователей; схемы аутентификации и др.

Шлюз прикладного уровня обладает следующими достоинствами:

- обеспечивает высокий уровень защиты локальной сети благодаря возможности выполнения большинства функций посредничества;
- защита на уровне приложений позволяет осуществлять большое количество дополнительных проверок, уменьшая тем самым ве-

роятность проведения успешных атак, основанных на недостатках программного обеспечения;
- при нарушении работоспособности прикладного шлюза блокируется сквозное прохождение пакетов между разделяемыми сетями, в результате безопасность защищаемой сети не снижается из-за возникновения отказов.

К недостаткам прикладного шлюза относятся:
- относительно высокая стоимость;
- довольно большая сложность самого МЭ, а также процедур его установки и конфигурирования;
- высокие требования к производительности и ресурсоемкости компьютерной платформы;
- отсутствие прозрачности для пользователей и снижение пропускной способности при реализации межсетевых взаимодействий.

10.2.4. Шлюз экспертного уровня

Для устранения такого существенного недостатка прикладных шлюзов, как отсутствие прозрачности для пользователей и снижение пропускной способности при реализации межсетевых взаимодействий, компании Check Point и ON Technology разработали технологию фильтрации пакетов, которую иногда называют *фильтрацией с контролем состояния соединения (Stateful Inspection)*, или фильтрацией экспертного уровня [7]. Такая фильтрация осуществляется на основе специальных методов многоуровневого анализа состояния пакетов SMLT (Stateful Multi-Layer Technique).

Эта гибридная технология позволяет отслеживать состояние сетевого соединения, перехватывая пакеты на сетевом уровне и извлекая из них информацию прикладного уровня, которая используется для контроля за соединением. Быстрое сравнение проходящих пакетов с известным состоянием (State) «дружественных» пакетов позволяет значительно сократить время обработки по сравнению с МЭ уровня приложений.

Межсетевые экраны, в основу функционирования которых положена описанная технология фильтрации, называют *МЭ экспертного уровня*. Такие МЭ сочетают в себе элементы экранирующих маршрутизаторов и прикладных шлюзов. Как и экранирующие маршрутизаторы, они обеспечивают фильтрацию пакетов по содержимому их заголовков сетевого и транспортного уровней модели OSI. МЭ экспертного уровня также выполняют все функции прикладного шлюза, касающиеся фильтрации пакетов на прикладном уровне модели OSI. Они оценивают содержимое каждого пакета в соответствии с заданной политикой безопасности.

Таким образом, МЭ экспертного уровня позволяют контролировать:
- каждый передаваемый пакет — на основе имеющейся таблицы правил;
- каждую сессию — на основе таблицы состояний;
- каждое приложение — на основе разработанных посредников.

Достоинством межсетевых экранов экспертного уровня является прозрачность для конечного пользователя, не требующая дополнительной настройки или изменения конфигурации клиентского программного обеспечения. Помимо прозрачности для пользователей и более высокой скорости обработки информационных потоков, к достоинствам межсетевых экранов экспертного уровня относится также то, что эти МЭ не изменяют IP-адресов проходящих через них пакетов. Это означает, что любой протокол прикладного уровня, использующий IP-адреса, будет корректно работать с этими МЭ без каких-либо изменений или специального программирования.

Поскольку данные МЭ допускают прямое соединение между авторизованным клиентом и компьютером внешней сети, они обеспечивают менее высокий уровень защиты. Поэтому на практике технология фильтрации экспертного уровня используется для повышения эффективности функционирования комплексных МЭ. Примерами комплексных МЭ, реализующих технологию фильтрации экспертного уровня, является FireWall-1 компании Check Point Software. Следует заметить, что термин Stateful Inspection, введенный компанией Check Point Software, стал таким популярным, что сейчас трудно найти межсетевой экран, который не относили бы к этой категории.

В настоящее время фильтрация экспертного уровня становится одной из функций новых маршрутизаторов. Например, компании Bay Networks и Check Point Software заключили партнерское соглашение с целью переноса разработанной Check Point Software архитектуры МЭ экспертного уровня на маршрутизаторы Bay Networks. Компания Cisco Systems разработала собственную технологию МЭ экспертного уровня и реализовала ее в продукте Cisco PIX Firewall.

10.2.5. Варианты исполнения межсетевых экранов

Существует два основных варианта исполнения межсетевых экранов — программный и программно-аппаратный. В свою очередь, программно-аппаратный вариант исполнения межсетевых экранов имеет две разновидности — в виде специализированного устройства и в виде модуля в маршрутизаторе или коммутаторе.

В настоящее время чаще используется программное решение, которое на первый взгляд выглядит более привлекательным. Это связано с тем, что для его применения достаточно, казалось бы, только приобрести программное обеспечение межсетевого экрана и установить его на любой компьютер, имеющийся в организации. Однако на практике далеко не всегда в организации находится свободный компьютер, да еще и удовлетворяющий достаточно высоким требованиям по системным ресурсам. Поэтому одновременно с приобретением программного обеспечения приобретается и компьютер для его установки. Потом следует процесс установки на компьютер операционной системы и ее настрой-

ка, что также требует времени и оплаты работы установщиков. И только после этого устанавливается и настраивается программное обеспечение системы обнаружения атак. Нетрудно заметить, что использование обычного персонального компьютера далеко не так просто, как кажется на первый взгляд.

Поэтому в последние годы значительно возрос интерес к программно-аппаратным решениям [7, 27]. Такие решения начинают постепенно вытеснять чисто программные системы. Все более широкое распространение стали получать специализированные программно-аппаратные решения (Security Appliance). Программно-аппаратный комплекс межсетевого экранирования обычно состоит из компьютера, а также функционирующих на нем операционной системы (ОС) и специального программного обеспечения. Следует отметить, что это специальное программное обеспечение часто называют firewall. Используемый компьютер должен быть достаточно мощным и физически защищенным, например находиться в специально отведенном и охраняемом помещении. Кроме того, он должен иметь средства защиты от загрузки ОС с несанкционированного носителя. Программно-аппаратные комплексы используют специализированные или обычные операционные системы (как правило, на базе FreeBSD, Linux или Microsoft Windows NT/2000), урезанные для выполнения заданных функций и удовлетворяющие ряду требований:

- иметь средства разграничения доступа к ресурсам системы;
- блокировать доступ к компьютерным ресурсам в обход предоставляемого программного интерфейса;
- запрещать привилегированный доступ к своим ресурсам из локальной сети;
- содержать средства мониторинга/аудита любых административных действий.

Специализированные программно-аппаратные решения обладают следующими достоинствами:

- *простотой внедрения в технологию обработки информации.* Такие средства поставляются уже с заранее установленной и настроенной операционной системой и защитными механизмами, поэтому необходимо только подключить их к сети, что выполняется в течение нескольких минут;
- *простотой управления.* Данные средства могут управляться с любой рабочей станции Windows 9x, NT, 2000 или UNIX. Взаимодействие консоли управления с устройством осуществляется либо по стандартным протоколам, например Telnet или SNMP, либо при помощи специализированных или защищенных протоколов, например SSH или SSL;
- *отказоустойчивостью и высокой доступностью.* Исполнение межсетевого экрана в виде специализированного программно-аппаратного комплекса позволяет реализовать механизмы обеспечения не только программной, но и аппаратной отказоустойчивости и высокой доступности;

- *высокой производительностью и надежностью.* За счет исключения из операционной системы всех ненужных сервисов и подсистем, программно-аппаратный комплекс работает более эффективно с точки зрения производительности и надежности;
- *специализацией на защите.* Решение только задач обеспечения сетевой безопасности не приводит к затратам ресурсов на выполнение других функций, например маршрутизации и т. п.

10.3. Схемы сетевой защиты на базе межсетевых экранов

При подключении корпоративной или локальной сети к глобальным сетям необходимо решать следующие задачи:

- защита корпоративной или локальной сети от несанкционированного удаленного доступа со стороны глобальной сети;
- сокрытие информации о структуре сети и ее компонентов от пользователей глобальной сети;
- разграничение доступа в защищаемую сеть из глобальной сети и из защищаемой сети в глобальную сеть.

Для эффективной защиты межсетевого взаимодействия система МЭ должна быть правильно установлена и сконфигурирована. Данный процесс состоит из следующих шагов:

- формирование политики межсетевого взаимодействия;
- выбор схемы подключения и настройка параметров функционирования межсетевого экрана.

10.3.1. Формирование политики межсетевого взаимодействия

Политика межсетевого взаимодействия является составной частью общей политики безопасности в организации. Политика межсетевого взаимодействия определяет требования к безопасности информационного обмена организации с внешним миром. Эта политика должна отражать два аспекта [7, 27]:

- политику доступа к сетевым сервисам;
- политику работы межсетевого экрана.

Политика доступа к сетевым сервисам определяет правила предоставления, а также использования всех возможных сервисов защищаемой компьютерной сети. В рамках данной политики должны быть заданы все сервисы, предоставляемые через межсетевой экран, и допустимые адреса клиентов для каждого сервиса. Кроме того, для пользователей должны быть указаны правила, описывающие, когда и какие пользователи каким сервисом и на каком компьютере могут воспользоваться.

Задаются также ограничения на методы доступа, например на использование протоколов SLIP (Serial Line Internet Protocol) и PPP (Point-to-Point Protocol). Ограничение методов доступа необходимо для того, чтобы пользователи не могли обращаться к запрещенным сервисам Интернета обходными путями. Правила аутентификации пользователей и компьютеров, а также условия работы пользователей вне локальной сети организации должны быть определены отдельно.

Для того чтобы межсетевой экран успешно защищал ресурсы организации, политика доступа пользователей к сетевым сервисам должна быть реалистичной. Реалистичной считается такая политика, при которой найден баланс между защитой сети организации от известных рисков и необходимым доступом пользователей к сетевым сервисам.

Политика работы межсетевого экрана задает базовый принцип управления межсетевым взаимодействием, положенный в основу функционирования МЭ. Может быть выбран один из двух таких принципов:

- запрещено все, что явно не разрешено;
- разрешено все, что явно не запрещено.

Фактически выбор принципа устанавливает, насколько «подозрительной» или «доверительной» должна быть система защиты. В зависимости от выбора решение может быть принято как в пользу безопасности в ущерб удобству использования сетевых сервисов, так и наоборот.

При выборе принципа «запрещено все, что явно не разрешено» межсетевой экран настраивается таким образом, чтобы блокировать любые явно не разрешенные межсетевые взаимодействия. Данный принцип соответствует классической модели доступа, используемой во всех областях информационной безопасности. Такой подход позволяет адекватно реализовать принцип минимизации привилегий, поэтому с точки зрения безопасности он является лучшим. Администратор безопасности должен на каждый тип разрешенного взаимодействия задавать одно и более правил доступа. Администратор не сможет по забывчивости оставить разрешенными какие-либо полномочия, так как по умолчанию они будут запрещены. Доступные лишние сервисы могут быть использованы во вред безопасности, что особенно характерно для закрытого и сложного программного обеспечения, в котором могут быть различные ошибки и некорректности. Принцип «запрещено все, что явно не разрешено», в сущности, является признанием факта, что незнание может причинить вред. Следует отметить, что правила доступа, сформулированные в соответствии с этим принципом, могут доставлять пользователям определенные неудобства.

При выборе принципа «разрешено все, что явно не запрещено» межсетевой экран настраивается таким образом, чтобы блокировать только явно запрещенные межсетевые взаимодействия. В этом случае повышается удобство использования сетевых сервисов со стороны пользователей, но снижается безопасность межсетевого взаимодействия. Пользователи имеют больше возможностей обойти межсетевой экран, например могут получить доступ к новым сервисам, не запре-

щаемым политикой (или даже не указанным в политике), или запустить неразрешенные сервисы на нестандартных портах TCP/UDP, которые не запрещены политикой. Администратор может учесть не все действия, которые запрещены пользователям. Ему приходится работать в режиме реагирования, предсказывая и запрещая те межсетевые взаимодействия, которые отрицательно воздействуют на безопасность сети. При реализации данного принципа внутренняя сеть оказывается менее защищенной от нападений хакеров. Поэтому производители межсетевых экранов обычно отказываются от использования данного принципа.

Межсетевой экран не является симметричным. Для него отдельно задаются правила, ограничивающие доступ из внутренней сети во внешнюю сеть, и наоборот. В общем случае работа межсетевого экрана основана на динамическом выполнении двух групп функций:

- фильтрации проходящих через него информационных потоков;
- посредничества при реализации межсетевых взаимодействий.

В зависимости от типа экрана эти функции могут выполняться с различной полнотой. Простые межсетевые экраны ориентированы на выполнение только одной из данных функций. Комплексные МЭ обеспечивают совместное выполнение указанных функций защиты. Собственная защищенность межсетевого экрана достигается с помощью тех же средств, что и защищенность универсальных систем [7].

Чтобы эффективно обеспечивать безопасность сети, комплексный МЭ обязан управлять всем потоком, проходящим через него, и отслеживать свое состояние. Для принятия управляющих решений по используемым сервисам МЭ должен получать, запоминать, выбирать и обрабатывать информацию, полученную от всех коммуникационных уровней и от других приложений.

Недостаточно просто проверять пакеты по отдельности. Информация о состоянии соединения, полученная из инспекции соединений в прошлом и других приложений, — главный фактор в принятии управляющего решения при попытке установления нового соединения. Для принятия решения могут учитываться как состояние соединения (полученное из прошлого потока данных), так и состояние приложения (полученное из других приложений). Полнота и правильность управления требуют, чтобы комплексный МЭ имел возможность анализа и использования следующих элементов:

- *информации о соединениях* — информации от всех семи уровней в пакете;
- *истории соединений* — информации, полученной от предыдущих соединений;
- *состояния уровня приложения* — информации о состоянии, полученной из других приложений. Например, аутентифицированному до настоящего момента пользователю можно предоставить доступ через МЭ только для авторизованных видов сервиса;
- *агрегирующих элементов* — вычислений разнообразных выражений, основанных на всех вышеперечисленных факторах.

10.3.2. Основные схемы подключения межсетевых экранов

При подключении корпоративной сети к глобальным сетям необходимо разграничить доступ в защищаемую сеть из глобальной и из защищаемой сети в глобальную, а также обеспечить защиту подключаемой сети от несанкционированного удаленного доступа со стороны глобальной сети. При этом организация заинтересована в сокрытии информации о структуре своей сети и ее компонентов от пользователей глобальной сети. Работа с удаленными пользователями требует установления жестких ограничений доступа к информационным ресурсам защищаемой сети.

У организации часто возникает потребность иметь в составе корпоративной сети нескольких сегментов с разными уровнями защищенности:

- свободно доступные сегменты (например, рекламный WWW-сервер);
- сегмент с ограниченным доступом (например, для доступа сотрудникам организации с удаленных узлов);
- закрытые сегменты (например, финансовая локальная подсеть организации).

Для подключения межсетевых экранов могут использоваться различные схемы, которые зависят от условий функционирования защищаемой сети, а также от количества сетевых интерфейсов и других характеристик используемых МЭ. Широкое распространение получили следующие схемы подключения межсетевых экранов:

- схемы защиты сети с использованием экранирующего маршрутизатора;
- схемы единой защиты локальной сети;
- схемы с защищаемой закрытой и незащищаемой открытой подсетями;
- схемы с раздельной защитой закрытой и открытой подсетей [7, 27].

Схема защиты с использованием экранирующего маршрутизатора. Межсетевой экран, основанный на фильтрации пакетов, является самым распространенным и наиболее простым в реализации. Он состоит из экранирующего маршрутизатора, расположенного между защищаемой сетью и потенциально враждебной открытой внешней сетью (рис. 10.9). Экранирующий маршрутизатор (пакетный фильтр) сконфигурирован для блокирования или фильтрации входящих и исходящих пакетов на основе анализа их адресов и портов.

Рис. 10.9. Межсетевой экран — экранирующий маршрутизатор

Компьютеры, находящиеся в защищаемой сети, имеют прямой доступ в сеть Интернет, в то время как бо́льшая часть доступа к ним из Интернета блокируется. Часто блокируются такие опасные службы, как X Windows, NIS и NFS. В принципе, экранирующий маршрутизатор может реализовать любую из политик безопасности, описанных ранее. Однако если маршрутизатор не фильтрует пакеты по порту источника и номеру входного и выходного порта, то реализация политики «запрещено все, что не разрешено в явной форме» может быть затруднена.

Межсетевые экраны, основанные на фильтрации пакетов, имеют те же недостатки, что и экранирующие маршрутизаторы, причем эти недостатки становятся более ощутимыми при ужесточении требований к безопасности защищаемой сети. Отметим некоторые из них:

- сложность правил фильтрации, в некоторых случаях совокупность этих правил может стать неуправляемой;
- невозможность полного тестирования правил фильтрации, это приводит к незащищенности сети от непротестированных атак;
- практически отсутствующие возможности регистрации событий, в результате администратору трудно определить, подвергался ли маршрутизатор атаке и скомпрометирован ли он.

Схемы подключения межсетевых экранов с несколькими сетевыми интерфейсами. Схемы защиты с МЭ с одним сетевым интерфейсом (рис. 10.10) недостаточно эффективны как с точки зрения безопасности, так и с позиций удобства конфигурирования. Они физически не разграничивают внутреннюю и внешнюю сети, а соответственно, не могут обеспечивать надежную защиту межсетевых взаимодействий. Настройка таких межсетевых экранов, а также связанных с ними маршрутизаторов представляет собой довольно сложную задачу, цена решения которой превышает стоимость замены МЭ с одним сетевым интерфейсом на МЭ с двумя или тремя сетевыми интерфейсами. Поэтому далее будут более подробно рассмотрены схемы подключения межсетевых экранов с двумя и тремя сетевыми интерфейсами.

Рис. 10.10. Защита локальной сети с помощью МЭ с одним сетевым интерфейсом

Защищаемую локальную сеть целесообразно представлять как совокупность закрытой и открытой подсетей. Здесь под *открытой подсетью* понимается подсеть, доступ к которой со стороны потенциально

враждебной внешней сети может быть полностью или частично открыт. В открытую подсеть могут, например, входить общедоступные WWW-, FTP- и SMTP-серверы, а также терминальный сервер с модемным пулом.

Среди множества возможных схем подключения МЭ типовыми являются следующие:

- схема единой защиты локальной сети;
- схема с защищаемой закрытой и незащищаемой открытой подсетями;
- схема с раздельной защитой закрытой и открытой подсетей.

Схема единой защиты локальной сети. Данная схема является наиболее простым решением (рис. 10.11), при котором МЭ целиком экранирует локальную сеть от потенциально враждебной внешней сети. Между маршрутизатором и МЭ имеется только один путь, по которому идет весь трафик. Данный вариант МЭ реализует политику безопасности, основанную на принципе «запрещено все, что явно не разрешено»; при этом пользователю недоступны все службы, кроме тех, для которых определены соответствующие полномочия. Обычно маршрутизатор настраивается таким образом, что МЭ является единственной видимой снаружи машиной.

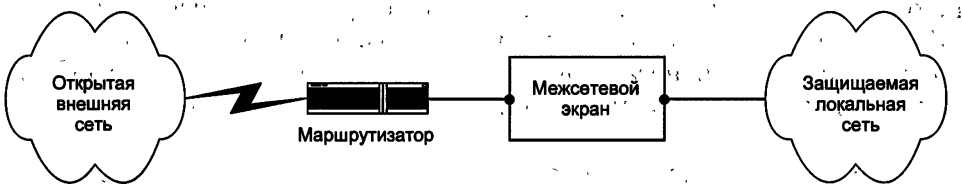


Рис. 10.11. Схема единой защиты локальной сети

Открытые серверы, входящие в локальную сеть, также будут защищены межсетевым экраном. Однако объединение серверов, доступных из внешней сети, вместе с другими ресурсами защищаемой локальной сети существенно снижает безопасность межсетевых взаимодействий. Поэтому данную схему подключения МЭ можно использовать лишь при отсутствии в локальной сети открытых серверов или когда имеющиеся открытые серверы делаются доступными из внешней сети только для ограниченного числа пользователей, которым можно доверять.

Поскольку межсетевой экран использует хост, то на нем могут быть установлены программы для усиленной аутентификации пользователей. Межсетевой экран может также протоколировать доступ, попытки зондирования и атак системы, что позволит выявить действия злоумышленников.

Для некоторых сетей может оказаться неприемлемой недостаточная гибкость схемы защиты на базе межсетевого экрана с двумя интерфейсами.

Схема с защищаемой закрытой и незащищаемой открытой подсетями. Если в составе локальной сети имеются общедоступные открытые серве-

ры, тогда их целесообразно вынести как открытую подсеть до межсетевого экрана (рис. 10.12). Данный способ обладает более высокой защищенностью закрытой части локальной сети, но обеспечивает пониженную безопасность открытых серверов, расположенных до межсетевого экрана.

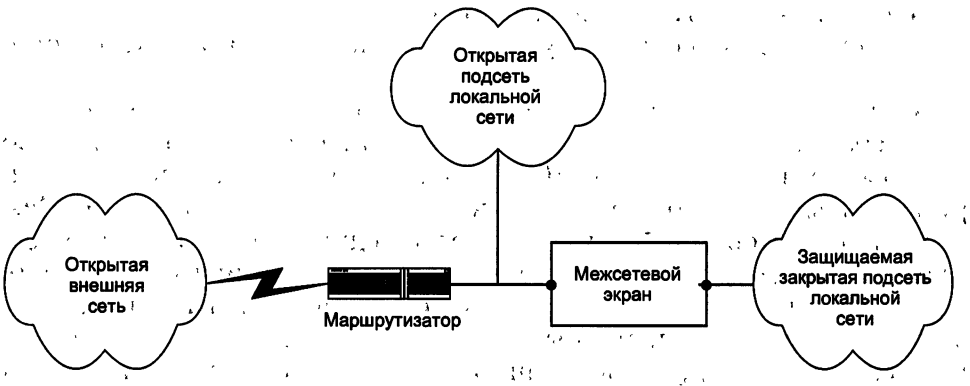


Рис. 10.12. Схема с защищаемой закрытой и незащищаемой открытой подсетями

Некоторые МЭ позволяют разместить эти серверы на себе. Однако такое решение не является лучшим с точки зрения безопасности самого МЭ и загрузки компьютера. Схему подключения МЭ с защищаемой закрытой подсетью и незащищаемой открытой подсетью целесообразно использовать лишь при невысоких требованиях по безопасности к открытой подсети.

Если же к безопасности открытых серверов предъявляются повышенные требования, тогда необходимо использовать схему с раздельной защитой закрытой и открытой подсетей.

Схемы с раздельной защитой закрытой и открытой подсетей. Такая схема может быть построена *на основе одного МЭ с тремя сетевыми интерфейсами* (рис. 10.13) или *на основе двух МЭ с двумя сетевыми интерфейсами* (рис. 10.14). В обоих случаях доступ к открытой и закрытой подсетям локальной сети возможен только через межсетевой экран. При этом доступ к открытой подсети не позволяет осуществить доступ к закрытой подсети.

Из этих двух схем бо́льшую степень безопасности межсетевых взаимодействий обеспечивает схема с двумя МЭ, каждый из которых образует отдельный эшелон защиты закрытой подсети. Защищаемая открытая подсеть здесь выступает в качестве экранирующей подсети.

Обычно экранирующую подсеть конфигурируют таким образом, чтобы обеспечить доступ к компьютерам подсети как из потенциально враждебной внешней сети, так и из закрытой подсети локальной сети. Однако прямой обмен информационными пакетами между внешней сетью и закрытой подсетью невозможен. При атаке системы с экранирующей подсетью необходимо преодолеть по крайней мере две независимые линии защиты, что является весьма сложной задачей. Средства

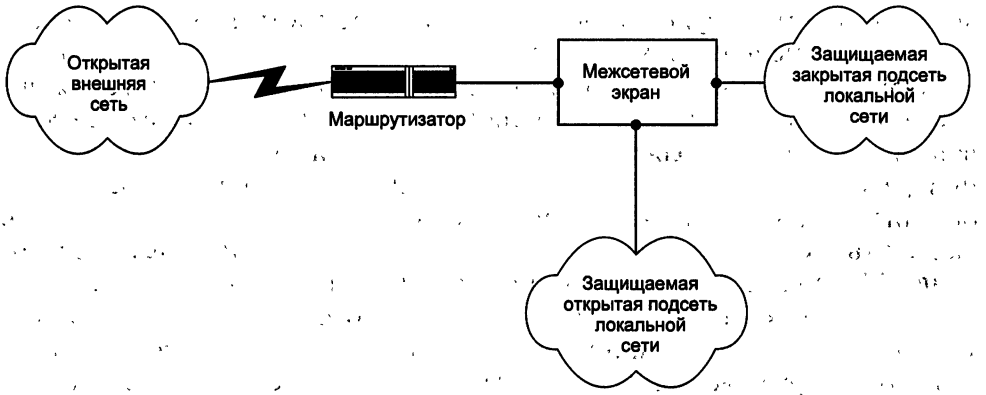


Рис. 10.13. Схема с раздельной защитой закрытой и открытой подсетей на основе одного МЭ с тремя сетевыми интерфейсами

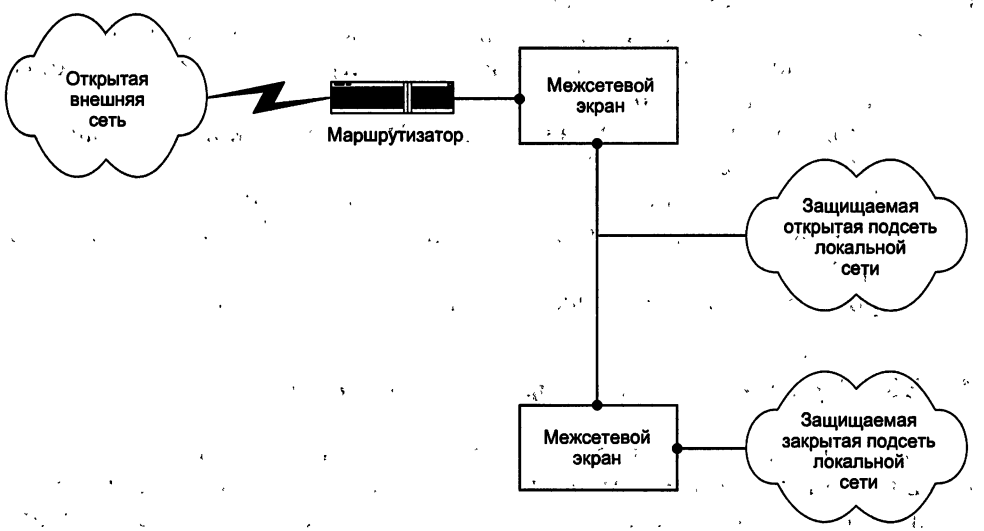


Рис. 10.14. Схема с раздельной защитой закрытой и открытой подсетей на основе двух МЭ с двумя сетевыми интерфейсами

мониторинга состояния межсетевых экранов позволяют практически всегда обнаружить подобную попытку, и администратор системы может своевременно предпринять необходимые действия по предотвращению несанкционированного доступа.

Следует обратить внимание на то, что работа удаленных пользователей, подключаемых через коммутируемые линии связи, также должна контролироваться в соответствии с политикой безопасности, проводимой в организации. Типовое решение этой задачи — установка сервера удаленного доступа (терминального сервера), который обладает необходимыми функциональными возможностями, например терминального сервера Annex компании Bay Networks. Терминальный сервер является системой с несколькими асинхронными портами и одним интерфейсом локальной сети. Обмен информацией между асинхронными портами и

локальной сетью осуществляется только после соответствующей аутентификации внешнего пользователя.

Подключение терминального сервера должно осуществляться таким образом, чтобы его работа выполнялась исключительно через межсетевой экран. Это позволяет достичь необходимой степени безопасности при работе удаленных пользователей с информационными ресурсами организации. Такое подключение возможно, если терминальный сервер включить в состав открытой подсети при использовании схем подключения МЭ с раздельной защитой открытой и закрытой подсетей.

Программное обеспечение терминального сервера должно предоставлять возможности администрирования и контроля сеансов связи через коммутируемые каналы. Модули управления современных терминальных серверов имеют достаточно развитые возможности обеспечения безопасности самого сервера и разграничения доступа клиентов и выполняют следующие функции:

- использование локального пароля на доступ к последовательному порту, на удаленный доступ по протоколу PPP, а также для доступа к административной консоли;
- использование запроса на аутентификацию с какой-либо машины локальной сети;
- использование внешних средств аутентификации;
- установка списка контроля доступа на порты терминального сервера;
- протоколирование сеансов связи через терминальный сервер.

10.3.3. Персональные и распределенные сетевые экраны

За последние несколько лет в структуре корпоративных сетей произошли определенные изменения. Если раньше границы таких сетей можно было четко очертить, то сейчас это практически невозможно. Еще недавно такая граница проходила через все маршрутизаторы или иные устройства (например, модемы), через которые осуществлялся выход во внешние сети. В удаленных офисах организации ситуация была схожей. С появлением новых сервисов и технологий, в частности мобильного доступа к ЛВС или использования беспроводных сегментов сети, понятие «периметр» начинает терять свое значение.

Наиболее уязвимым местом корпоративной сети являются рабочие станции конечных пользователей, находящиеся за пределами защищаемого периметра, которые имеют, как правило, низкий уровень защиты. Все традиционные межсетевые экраны построены так, что защищаемые пользователи и ресурсы должны находиться под их защитой с внутренней стороны корпоративной или локальной сети, что является невозможным для мобильных пользователей.

Следует также упомянуть о такой проблеме, как обеспечение внутренней безопасности сети. Технология обеспечения внутренней безопасности отличается от технологии защиты периметра. Для отражения

атак из внешней по отношению к ЛВС сети существуют весьма эффективные средства, которые помогают защитить рабочие станции пользователей от атак и других подозрительных действий, направленных на получение конфиденциальной информации. А вот отследить и предотвратить атаки, организуемые из локальной сети, по-прежнему достаточно сложно. И опасности, связанные с внутренней безопасностью, постоянно растут.

Для решения указанных проблем предложены следующие подходы: применение персональных и распределенных межсетевых экранов и использование возможностей виртуальных частных сетей VPN, а также технологии Total Access Protection (Check Point), Network Admission Control (Cisco), Network Access Protection («Майкрософт») и т. п., которые направлены на установление жесткого контроля защищенности конечных пользователей.

Для индивидуальных пользователей представляет интерес *технология персонального сетевого экранирования*. В этом случае сетевой экран устанавливается на защищаемый персональный компьютер. Такой экран, называемый персональным экраном компьютера (Personal Firewall) или системой сетевого экранирования, контролирует весь исходящий и входящий трафик независимо от всех прочих системных защитных средств. При экранировании отдельного компьютера поддерживается доступность сетевых сервисов, но уменьшается нагрузка, индуцированная внешней активностью. В результате снижается уязвимость внутренних сервисов защищаемого таким образом компьютера, поскольку сторонний злоумышленник должен сначала преодолеть экран, где защитные средства сконфигурированы особенно тщательно и жестко. Для защиты рабочего места пользователя необходимо иметь, кроме персонального МЭ, антивирусное ПО с актуальными сигнатурами, защиту доступа в корпоративную сеть через VPN.

В качестве примера персонального сетевого экрана можно указать межсетевой экран Windows Firewall, который служит первой линией защиты персонального компьютера от различного рода вредоносных программ. Начиная с версии Windows XP Service Pack 2 межсетевой экран Windows Firewall включен в ОС по умолчанию и защищает компьютер с момента загрузки операционной системы. Он удобен в использовании, легко настраивается, имеет простой интерфейс и практически незаметен при работе. Если в системе Windows XP Service Pack 2 межсетевой экран фильтрует только входящий трафик, то в операционной системе Windows Vista межсетевой экран является двусторонним, позволяя осуществлять фильтрацию как входящего, так и исходящего трафика. Межсетевой экран Windows Firewall может блокировать весь входящий трафик до тех пор, пока на компьютер не будут установлены все последние пакеты обновлений.

При надлежащей настройке межсетевой экран Windows Firewall не позволяет большинству вредоносных программ проникать в систему, обеспечивая защиту от хакеров, вирусов и компьютерных червей, которые пытаются получить доступ к компьютеру через Интернет.

Распределенный межсетевой экран представляет собой централизованно управляемую совокупность сетевых мини-экранов, защищающих отдельные компьютеры сети. При построении распределенных систем МЭ их функциональные компоненты распределяются по узлам сети и могут обладать различной функциональностью. При обнаружении подозрительных на атаку признаков управляющие модули распределенного МЭ могут адаптивно изменять конфигурацию, состав и расположение компонентов.

Главное отличие распределенного межсетевого экрана от персонального экрана заключается в наличии у распределенного межсетевого экрана функции централизованного управления. Если персональные сетевые экраны управляются только с того компьютера, на котором они установлены, и идеально подходят для домашнего применения, то распределенные межсетевые экраны могут управляться централизованно, с единой консоли управления, установленной в главном офисе организации. Такие отличия позволили некоторым производителям выпускать свои решения МЭ в двух версиях:

- персональной (для индивидуальных пользователей);
- распределенной (для корпоративных пользователей).

В современных условиях более 60 % различных атак и попыток доступа к информации осуществляется изнутри локальных сетей, поэтому классический «периметровый» подход к созданию системы защиты корпоративной сети становится недостаточно эффективным. Корпоративную сеть можно считать действительно защищенной от НСД только при наличии в ней как средств защиты точек входа со стороны Интернета, так и решений, обеспечивающих безопасность отдельных компьютеров, корпоративных серверов и фрагментов локальной сети предприятия. Решения на основе распределенных или персональных межсетевых экранов наилучшим образом обеспечивают безопасность отдельных компьютеров, корпоративных серверов и фрагментов локальной сети предприятия [69].

10.3.4. Примеры современных межсетевых экранов

К лидерам производства межсетевых экранов можно отнести три компании — Cisco, Check Point и Juniper, причем с существенным отрывом на мировом рынке лидирует компания Cisco. Рассмотрим подробнее возможности межсетевых экранов компании Cisco.

Компания Cisco предлагает два вида межсетевых экранов Cisco PIX Firewall и Cisco IOS Firewall. Выбор между ними осуществляется исходя из индивидуальных потребностей заказчика — межсетевой экран Cisco PIX Firewall обеспечивает решение на базе отдельного специализированного устройства, а при использовании Cisco IOS Firewall решение оказывается интегрированным в инфраструктуру сети. Использование межсетевых экранов Cisco в сочетании с многоуровневой стратегией защиты позволяет реализовать более мощную архитектуру сетевой безопасности.

Программно-аппаратный межсетевой экран CISCO PIX FIREWALL

Программно-аппаратный межсетевой экран Cisco Pix Firewall обеспечивает многоуровневую защиту, используя широкий набор интегрированных защитных возможностей, включающих контроль состояния с помощью алгоритма адаптивной защиты Adaptive Security Algorithm и глубокий анализ сетевых и прикладных протоколов с помощью механизма Deep Packet Inspection.

Широкий спектр моделей Cisco Pix Firewall, ориентированных на защиту различных категорий заказчиков, начиная от надомных пользователей и предприятий малого/среднего бизнеса и заканчивая крупными корпорациями и операторами связи, обеспечивает безопасность, производительность и надежность сетей любого масштаба.

Основные возможности:

- производительность до 1,67 Гбит/с;
- поддержка технологий VPN;
- встроенная система обнаружения атак;
- фильтрация URL и блокирование ПО для Instant Messaging (IM) и P2P;
- поддержка протокола GTP/GPRS;
- прозрачный МСЭ второго уровня;
- виртуальные МСЭ;
- отказоустойчивость (включая поддержание VPN-туннелей);
- сокрытие топологии защищаемой сети с помощью трансляции адресов (NAT) и портов (PAT);
- контроль всего спектра протоколов для IP-телефонии и мультимедийных средств — H.323, SIP, SCCP, MGCP, RTSP и т. д.;
- поддержка IPv6.

Программный межсетевой экран CISCO IOS FIREWALL

Программное обеспечение Cisco IOS Firewall — это межсетевой экран с контролем состояния, интегрированный в операционную систему Cisco IOS и поддерживаемый на широком спектре моделей маршрутизаторов Cisco 800, 1600, 1700, 1800, 2500, 2600, 2800, 3600, 3700, 3800, 7100, 7200, 7400, 7500, 7600.

Cisco IOS Firewall использует эффективный механизм, называемый Context Based Access Control (CBAC), который позволяет контролировать информационные потоки, проходящие через маршрутизатор, на всех уровнях, начиная с сетевого и заканчивая прикладным. На всех уровнях фильтрация осуществляется динамически, основываясь на направлении трафика, состоянии соединения и информации о предыдущих пакетах и сессиях, обработанных маршрутизатором с Cisco IOS Firewall.

Основные возможности:

- поддержка большого числа протоколов, включая IPv6, в том числе и для мультимедийных средств;

- поддержка различных механизмов аутентификации — RADIUS, TACACS+ и т. д.;
- контроль доступа по времени;
- тесная интеграция с механизмами обнаружения атак, контроля качества (QoS) и построения VPN;
- поддержка различных политик и списков контроля доступа для разных интерфейсов;
- поддержка анализа протоколов на нестандартных портах;
- трансляция сетевых адресов;
- поддержка отказоустойчивости за счет динамической смены маршрута на резервный маршрутизатор;
- механизм прозрачности МСЭ (функционирование на канальном уровне);
- расширенная регистрация событий безопасности;
- фильтрация и блокирование трафика интернет-пейджеров, пиринговых приложений (P2P) и других сетевых приложений благодаря гибкому анализу на прикладном уровне;
- определяемые пользователем и расширяемые политики проверки объектов протокола HTTP (длина URL, заголовки HTTP и др.);
- возможность использования конфигурации на основе CPL (Class-based Policy Language) для защиты от уязвимостей и HTTP-атак;
- предотвращение DoS-атак на основе сессионных политик и политики контроля входного потока.

10.3.5. Тенденции развития межсетевых экранов

Современные межсетевые экраны существенно отличаются от классических прототипов начала 1990-х годов. Если раньше МЭ был предназначен только для разграничения доступа между Интернетом и внутренней сетью, то сегодня появились новые области его применения:

- сегментация сети с различными требованиями по безопасности;
- защита центров обработки данных;
- защита серверов приложений и т. д.

Тенденции дальнейшего развития межсетевых экранов можно увидеть в некоторых продвинутых решениях современных МЭ.

Применение в межсетевых экранах технологии *Deep Packet Inspection* позволило проводить более глубокий анализ пропускаемого через МЭ трафика на предмет обнаружения различных нарушений и атак. Технология *Deep Packet Inspection* позволила вывести межсетевые экраны на качественно новый уровень и защитить приложения и сервисы, ранее считавшиеся незащищенными, например технологию IP-телефонии.

Параллельно с МЭ с функцией *Deep Packet Inspection* стали появляться межсетевые экраны приложений (Application Firewall) — узкоспециализированные решения, которые ориентировались на защиту от-

дельных приложений или сервисов на прикладном уровне эталонной модели OSI.

Современные межсетевые экраны могут выполнять не только разграничение доступа между Интернетом и внутренней сетью, но и осуществлять глубокий анализ содержимого трафика, подключая ряд дополнительных подсистем предотвращения атак IPS (Intrusion Prevention), антивирусной защиты, контроля содержимого и др. Существуют межсетевые экраны со встроенной системой построения межофисных VPN.

Неотъемлемыми свойствами современных корпоративных межсетевых экранов стали централизованное управление, инспекция разных сетевых и прикладных протоколов, поддержка NAT, интеграция с различными серверами аутентификации, фильтрация URL и т. д.

Изменилась платформа, на которой реализуется межсетевой экран. Если раньше это было преимущественно программное решение, то постепенно произошел сдвиг в сторону аппаратной фильтрации трафика, что позволяет реализовать более скоростную и надежную обработку информационных потоков.

Аппаратные межсетевые экраны могут быть выполнены как в программно-аппаратном варианте, так и в виде специальных модулей, интегрируемых в маршрутизаторы и коммутаторы.

Появляются межсетевые экраны, ориентированные на защиту широко распространяющихся приложений для электронной коммерции на базе веб-сервисов. В существующих продуктах обеспечивается поддержка IP-телефонии, видеоконференц-связи, систем Telepresence. Поэтому в ближайшие годы можно ожидать развития межсетевых экранов, поднявшихся с уровня сети на прикладной.

Важной тенденцией, влияющей на развитие межсетевых экранов, является их более тесная интеграция с другими решениями по информационной безопасности. Пользователи предпочитают иметь одно устройство, решающее весь комплекс задач по защите сети и при этом объединяющее в себе решения производителей-лидеров по каждому из направлений сетевой безопасности.

Если интегрировать в одном устройстве сразу несколько защитных решений, то можно получить многофункциональное защитное устройство UTM (Unified Threat Management), которое позволяет сократить издержки и при этом обеспечить высокий уровень защиты за счет тесной интеграции таких защитных технологий, как межсетевой экран, система предотвращения атак, VPN, антивирус, антиспам, защита от шпионского ПО, контроль URL и т. п.

Подобные устройства UTM начали внедряться в филиалах, отделениях и иных удаленных площадках, для которых требования по безопасности те же, что и для центрального офиса, а выделяемых денег недостаточно на несколько отдельных устройств защиты. Эти решения постепенно вытесняют отдельные межсетевые экраны, IPS и др.

Возможно, и в центральных офисах будут устанавливаться такие интегрированные решения. Хотя такие решения противоречат важному

принципу безопасности «не класть все яйца в одну корзину», но в условиях финансовых затруднений лучше установить одно многофункциональное защитное устройство, чем не иметь совсем ничего.

Вопросы для самоконтроля

1. Сформулируйте понятия «межсетевое экранирование» и «межсетевой экран».
2. Объясните суть фильтрации информационного потока межсетевым экраном.
3. Какие параметры могут использоваться в качестве критериев анализа информационного потока?
4. Какие варианты решений принимаются при интерпретации правил фильтрации информационного потока?
5. Что представляют собой функции посредничества МЭ и программы-посредники? Перечислите функции, которые могут выполнять программы-посредники.
6. Назовите дополнительные возможности МЭ. Объясните суть трансляции внутренних сетевых адресов для исходящих пакетов сообщений.
7. Опишите особенности функционирования экранирующего маршрутизатора (пакетного фильтра).
8. Опишите особенности функционирования межсетевых экранов экспертного уровня. Как выполняется фильтрация пакетов с контролем состояния соединения?
9. Укажите достоинства программно-аппаратного варианта исполнения межсетевых экранов.
10. Сформулируйте принципы формирования политики межсетевого взаимодействия, реализуемой системой МЭ.
11. Назовите основные схемы подключения межсетевых экранов. Опишите функционирование схемы с защищаемой закрытой и незащищаемой открытой подсетями.
12. Расскажите о тенденциях дальнейшего развития межсетевых экранов.

Глава 11
ВИРТУАЛЬНЫЕ ЗАЩИЩЕННЫЕ СЕТИ VPN

Задача создания компьютерной сети предприятия в пределах одного здания может быть решена относительно легко, потому что обычно компании являются владельцами или арендаторами зданий и оборудования. Однако современная инфраструктура корпораций включает в себя географически распределенные подразделения самой корпорации, ее партнеров, клиентов и поставщиков. Создание защищенной корпоративной сети, включающей офисы, которые разнесенны на много километров и расположенные в разных городах или странах, — существенно более сложная задача.

В последнее десятилетие в связи с бурным развитием Интернета и сетей коллективного доступа в мире произошел качественный скачок в распространении и доступности информации. Пользователи получили дешевые и доступные каналы связи. Стремясь к экономии средств, предприятия хотят использовать такие каналы для передачи критичной коммерческой и управленческой информации.

Для эффективного противодействия сетевым атакам и обеспечения возможности активного и безопасного использования в бизнесе открытых сетей в начале 1990-х годов родилась и активно развивается концепция построения виртуальных частных сетей — VPN (Virtual Private Network).

11.1. Концепция построения виртуальных защищенных сетей VPN

В основе концепции построения виртуальных сетей VPN лежит достаточно простая идея: если в глобальной сети имеются два узла, которым нужно обменяться информацией, тогда между этими двумя узлами необходимо построить виртуальный защищенный туннель для обеспечения конфиденциальности и целостности информации, передаваемой через открытые сети; доступ к этому виртуальному туннелю должен быть чрезвычайно затруднен всем возможным активным и пассивным внешним наблюдателям.

Преимущества, получаемые компанией от создания таких виртуальных туннелей, заключаются прежде всего в значительной экономии финансовых средств, поскольку в этом случае компания может отказаться

от построения или аренды дорогих выделенных каналов связи для создания собственных интранет/экстранет-сетей и использовать для этого дешевые интернет-каналы, надежность и скорость передачи которых сегодня не уступает выделенным линиям. Очевидная экономическая эффективность от внедрения VPN-технологий стимулирует предприятия к активному их внедрению.

11.1.1. Основные понятия и функции сети VPN

При подключении корпоративной локальной сети к открытой сети возникают угрозы безопасности двух основных типов:

- несанкционированный доступ к внутренним ресурсам корпоративной локальной сети, получаемый злоумышленником в результате несанкционированного входа в эту сеть;
- несанкционированный доступ к корпоративным данным в процессе их передачи по открытой сети.

Обеспечение безопасности информационного взаимодействия локальных сетей и отдельных компьютеров через открытые сети, в частности через сеть Интернет, возможно путем эффективного решения следующих задач:

- защиты подключенных к открытым каналам связи локальных сетей и отдельных компьютеров от несанкционированных действий со стороны внешней среды;
- защиты информации в процессе ее передачи по открытым каналам связи.

Как уже отмечалось ранее, для защиты локальных сетей и отдельных компьютеров от несанкционированных действий со стороны внешней среды обычно используют межсетевые экраны, поддерживающие безопасность информационного взаимодействия путем фильтрации двустороннего потока сообщений, а также выполнения функций посредничества при обмене информацией. Межсетевой экран располагают на стыке между локальной и открытой сетью. Для защиты отдельного удаленного компьютера, подключенного к открытой сети, на этом компьютере устанавливают программное обеспечение сетевого экрана, и такой сетевой экран называется персональным.

Защита информации в процессе ее передачи по открытым каналам основана на использовании виртуальных защищенных сетей VPN. Виртуальной защищенной сетью VPN называют объединение локальных сетей и отдельных компьютеров через открытую внешнюю среду передачи информации в единую виртуальную корпоративную сеть, обеспечивающую безопасность циркулирующих данных. Виртуальная защищенная сеть VPN формируется путем построения виртуальных защищенных каналов связи, создаваемых на базе открытых каналов связи общедоступной сети. Эти виртуальные защищенные каналы связи называются туннелями VPN. Сеть VPN позволяет с помощью туннелей VPN соединить центральный офис, офисы филиалов, офисы бизнес-

партнеров и удаленных пользователей и безопасно передавать информацию через Интернет (рис. 11.1).

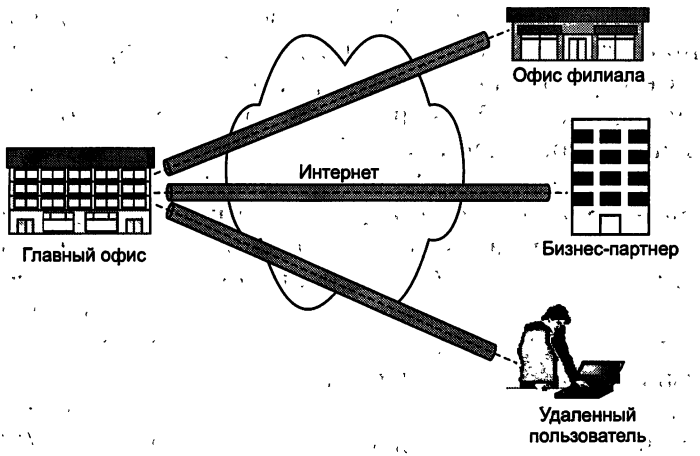


Рис. 11.1. Виртуальная защищенная сеть VPN

Туннель VPN представляет собой соединение, проведенное через открытую сеть, по которому передаются криптографически защищенные пакеты сообщений виртуальной сети. Защита информации в процессе ее передачи по туннелю VPN основана на выполнении следующих функций:

- аутентификация взаимодействующих сторон;
- криптографическое закрытие (шифрование) передаваемых данных;
- проверка подлинности и целостности доставляемой информации.

Для этих функций характерна взаимосвязь. При реализации этих функций используются криптографические методы защиты информации. Эффективность такой защиты обеспечивается за счет совместного использования симметричных и асимметричных криптографических систем. Туннель VPN, формируемый устройствами VPN, обладает свойствами защищенной выделенной линии, причем эта защищенная выделенная линия развертывается в рамках общедоступной сети, например Интернета. Устройства VPN могут играть в виртуальных частных сетях роль VPN-клиента, VPN-сервера или шлюза безопасности VPN.

VPN-клиент представляет собой программный или программно-аппаратный комплекс, выполняемый обычно на базе персонального компьютера. Его сетевое программное обеспечение модифицируется для выполнения шифрования и аутентификации трафика, которым это устройство обменивается с другими VPN-клиентами, VPN-серверами или шлюзами безопасности VPN. Обычно реализация VPN-клиента представляет собой программное решение, дополняющее стандартную операционную систему — Windows NT/2000/XP/Vista или UNIX.

VPN-сервер представляет собой программный или программно-аппаратный комплекс, устанавливаемый на компьютере, выполняющем функции сервера. VPN-сервер обеспечивает защиту серверов от не-

санкционированного доступа из внешних сетей, а также организацию защищенных соединений (ассоциаций) с отдельными компьютерами и с компьютерами из сегментов локальных сетей, защищенных соответствующими VPN-продуктами. VPN-сервер является функциональным аналогом продукта VPN-клиент для серверных платформ. Он отличается прежде всего расширенными ресурсами для поддержания множественных соединений с VPN-клиентами. VPN-сервер может поддерживать защищенные соединения с мобильными пользователями.

Шлюз безопасности VPN (*Security Gateway*) — это сетевое устройство, подключаемое к двум сетям, которое выполняет функции шифрования и аутентификации для многочисленных хостов, расположенных за ним. Размещение шлюза безопасности VPN выполняется таким образом, чтобы через него проходил весь трафик, предназначенный для внутренней корпоративной сети. Сетевое соединение шлюза VPN прозрачно для пользователей позади шлюза, оно представляется им выделенной линией, хотя на самом деле прокладывается через открытую сеть с коммутацией пакетов. Адрес шлюза безопасности VPN указывается как внешний адрес входящего туннелируемого пакета, а внутренний адрес пакета является адресом конкретного хоста позади шлюза. Шлюз безопасности VPN может быть реализован в виде отдельного программного решения, отдельного аппаратного устройства, а также в виде маршрутизатора или межсетевого экрана, дополненного функциями VPN.

Открытая внешняя среда передачи информации включает как каналы скоростной передачи данных, в качестве которой используется сеть Интернет, так и более медленные общедоступные каналы связи, для которых обычно применяются каналы телефонной сети. Эффективность виртуальной частной сети VPN определяется степенью защищенности информаций, циркулирующей по открытым каналам связи. Для безопасной передачи данных через открытые сети широко используют инкапсуляцию и туннелирование. С помощью методики туннелирования пакеты данных передаются через общедоступную сеть как по обычному двухточечному соединению. Между каждой парой отправитель—получатель данных устанавливается своеобразный туннель — логическое соединение, позволяющее инкапсулировать данные одного протокола в пакеты другого.

Суть туннелирования состоит в том, чтобы инкапсулировать, т. е. «упаковать» передаваемую порцию данных, вместе со служебными полями, в новый «конверт». При этом пакет протокола более низкого уровня помещается в поле данных пакета протокола более высокого или такого же уровня. Следует отметить, что туннелирование само по себе не защищает данные от несанкционированного доступа или искажения, но благодаря туннелированию появляется возможность полной криптографической защиты инкапсулируемых исходных пакетов. Чтобы обеспечить конфиденциальность передаваемых данных, отправитель шифрует исходные пакеты, упаковывает их во внешний пакет с новым IP-заголовком и отправляет его по транзитной сети (рис. 11.2).

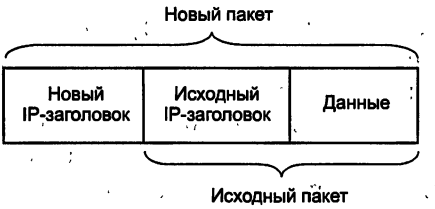


Рис. 11.2. Пример пакета, подготовленного для туннелирования

Особенностью туннелирования является то, что эта технология позволяет зашифровать исходный пакет целиком вместе с заголовком, а не только его поле данных. Это важно, поскольку некоторые поля заголовка содержат информацию, которая может быть использована злоумышленником. В частности, из заголовка исходного пакета можно извлечь сведения о внутренней структуре сети — данные о количестве подсетей и узлов и их IP-адресах. Злоумышленник может использовать такую информацию при организации атак на корпоративную сеть. Исходный пакет с зашифрованным заголовком не может быть использован для организации транспортировки по сети. Поэтому для защиты исходного пакета применяют его инкапсуляцию и туннелирование. Исходный пакет зашифровывают полностью вместе с заголовком и затем этот зашифрованный пакет помещают в другой внешний пакет с открытым заголовком. Для транспортировки данных по открытой сети используются открытые поля заголовка внешнего пакета.

По прибытии в конечную точку защищенного канала из внешнего пакета извлекают внутренний исходный пакет, расшифровывают его и используют его восстановленный заголовок для дальнейшей передачи по внутренней сети (рис. 11.3).

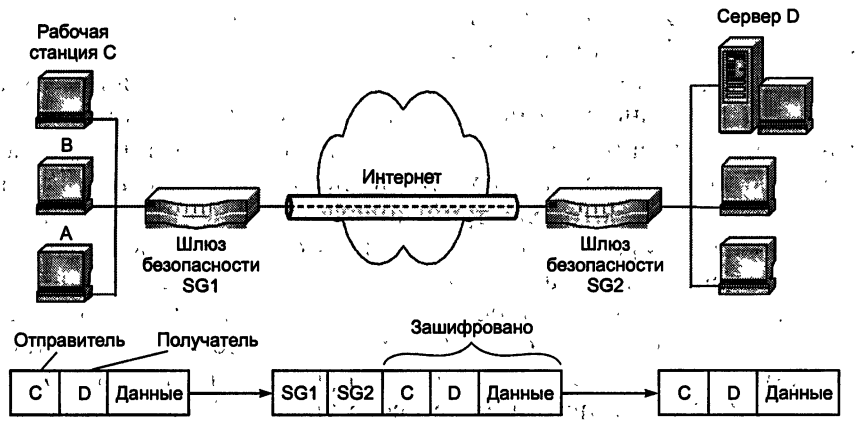


Рис. 11.3. Схема виртуального защищенного туннеля

Туннелирование может быть использовано для защиты не только конфиденциальности содержимого пакета, но и его целостности и аутентичности, при этом электронную цифровую подпись можно распространить на все поля пакета.

В дополнение к сокрытию сетевой структуры между двумя точками туннелирование может также предотвратить возможный конфликт адресов между двумя локальными сетями. При создании локальной сети, не связанной с Интернетом, компания может использовать любые IP-адреса для своих сетевых устройств и компьютеров. При объединении ранее изолированных сетей эти адреса могут начать конфликтовать друг с другом и с адресами, которые уже используются в Интернете. Инкапсуляция пакетов решает эту проблему, поскольку позволяет скрыть первоначальные адреса и добавить новые адреса, уникальные в пространстве IP-адресов Интернета, которые затем используются для пересылки данных по разделяемым сетям. Сюда же входит задача настройки IP-адреса и других параметров для мобильных пользователей, подключающихся к локальной сети.

Механизм туннелирования широко применяется в различных протоколах формирования защищенного канала. Обычно туннель создается только на участке открытой сети, где существует угроза нарушения конфиденциальности и целостности данных, например между точкой входа в открытый Интернет и точкой входа в корпоративную сеть. При этом для внешних пакетов используются адреса пограничных маршрутизаторов, установленных в этих двух точках, а внутренние адреса конечных узлов содержатся во внутренних исходных пакетах в защищенном виде. Следует отметить, что сам механизм туннелирования не зависит от того, с какой целью применяется туннелирование. Туннелирование может применяться не только для обеспечения конфиденциальности и целостности всей передаваемой порции данных, но и для организации перехода между сетями с разными протоколами (например, IPv4 и IPv6). Туннелирование позволяет организовать передачу пакетов одного протокола в логической среде, использующей другой протокол. В результате появляется возможность решить проблемы взаимодействия нескольких разнотипных сетей, начиная с необходимости обеспечения целостности и конфиденциальности передаваемых данных и заканчивая преодолением несоответствий внешних протоколов или схем адресации.

Реализацию механизма туннелирования можно представить как результат работы протоколов трех типов: протокола-«пассажира», несущего протокола и протокола туннелирования. Например, в качестве протокола-«пассажира» может быть использован транспортный протокол IPX, переносящий данные в локальных сетях филиалов одного предприятия. Наиболее распространенным вариантом несущего протокола является протокол IP сети Интернет. В качестве протоколов туннелирования могут быть использованы протоколы канального уровня PPTP и L2TP, а также протокол сетевого уровня IPSec. Благодаря туннелированию становится возможным сокрытие инфраструктуры Интернета от VPN-приложений.

Туннели VPN могут создаваться для различных типов конечных пользователей — либо это локальная сеть LAN (Local Area Network) с шлюзом безопасности, либо отдельные компьютеры удаленных и мобильных пользователей. Для создания виртуальной частной сети круп-

ного предприятия нужны VPN-шлюзы, VPN-серверы и VPN-клиенты. VPN-шлюзы целесообразно использовать для защиты локальных сетей предприятия, VPN-серверы и VPN-клиенты применяют для организации защищенных соединений удаленных и мобильных пользователей с корпоративной сетью через Интернет.

11.1.2. Варианты построения виртуальных защищенных каналов

Безопасность информационного обмена необходимо обеспечивать как при объединении локальных сетей, так и в случае доступа к локальным сетям удаленных или мобильных пользователей [63]. При проектировании VPN обычно рассматриваются две основные схемы:

- виртуальный защищенный канал между локальными сетями (канал ЛВС—ЛВС);
- виртуальный защищенный канал между узлом и локальной сетью (канал клиент—ЛВС) — рис. 11.4.

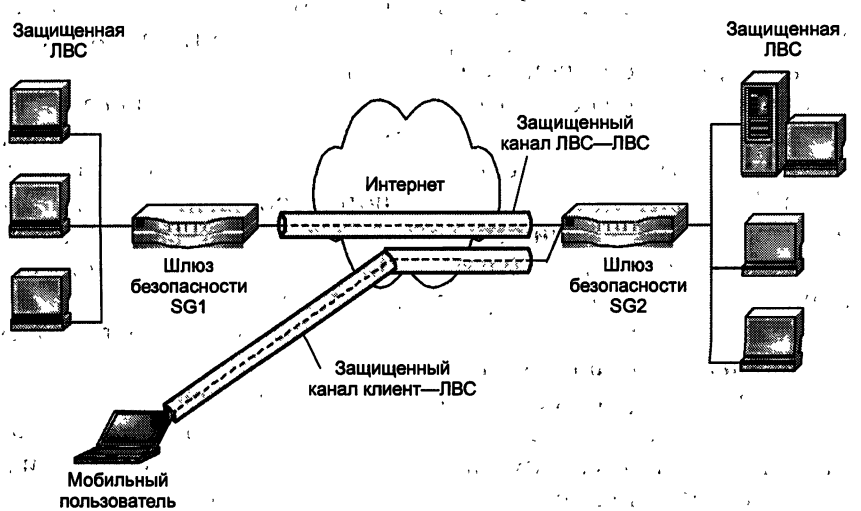


Рис. 11.4. Виртуальные защищенные каналы типа ЛВС—ЛВС и клиент—ЛВС

Первая схема соединения позволяет заменить дорогостоящие выделенные линии между отдельными офисами и создать постоянно доступные защищенные каналы между ними. В этом случае шлюз безопасности служит интерфейсом между туннелем и локальной сетью, при этом пользователи локальных сетей используют туннель для общения друг с другом. Многие компании используют данный вид VPN в качестве замены или дополнения к имеющимся соединениям глобальной сети, таким как Frame Relay.

Вторая схема защищенного канала VPN предназначена для установления соединений с удаленными или мобильными пользователями. Создание туннеля инициирует клиент (удаленный пользователь). Для

связи со шлюзом, защищающим удаленную сеть, он запускает на своем компьютере специальное клиентское программное обеспечение. Этот вид VPN заменяет собой коммутируемые соединения и может использоваться наряду с традиционными методами удаленного доступа.

Существует ряд вариантов схем виртуальных защищенных каналов. В принципе, любой из двух узлов виртуальной корпоративной сети, между которыми формируется виртуальный защищенный канал, может принадлежать конечной или промежуточной точке защищаемого потока сообщений.

С точки зрения обеспечения информационной безопасности лучшим является вариант, при котором конечные точки защищенного туннеля совпадают с конечными точками защищаемого потока сообщений. В этом случае обеспечивается защищенность канала вдоль всего пути следования пакетов сообщений. Однако такой вариант ведет к децентрализации управления и избыточности ресурсных затрат. В этом случае необходима установка средств создания VPN на каждом клиентском компьютере локальной сети. Это усложняет централизованное управление доступом к компьютерным ресурсам и не всегда оправдано экономически. Отдельное администрирование каждого клиентского компьютера с целью конфигурирования в нем средств защиты является достаточно трудоемкой процедурой в большой сети.

Если внутри локальной сети, входящей в виртуальную сеть, не требуется защита трафика, тогда в качестве конечной точки защищенного туннеля можно выбрать межсетевой экран или пограничный маршрутизатор этой локальной сети. Если же поток сообщений внутри локальной сети должен быть защищен, тогда в качестве конечной точки туннеля в этой сети должен выступать компьютер, который участвует в защищенном взаимодействии. При доступе к локальной сети удаленного пользователя компьютер этого пользователя должен быть конечной точкой виртуального защищенного канала.

Достаточно распространенным является вариант, когда защищенный туннель прокладывается только внутри открытой сети с коммутацией пакетов, например внутри Интернета. Этот вариант отличается удобством применения, но обладает сравнительно низкой безопасностью. В качестве конечных точек такого туннеля обычно выступают провайдеры Интернета или пограничные маршрутизаторы (межсетевые экраны) локальной сети.

При объединении локальных сетей туннель формируется только между пограничными провайдерами Интернета или маршрутизаторами (межсетевыми экранами) локальной сети. При удаленном доступе к локальной сети туннель создается между сервером удаленного доступа провайдера Интернета, а также пограничным провайдером Интернета или маршрутизатором (межсетевым экраном) локальной сети.

Построенные по данному варианту виртуальные корпоративные сети обладают хорошей масштабируемостью и управляемостью. Сформированные защищенные туннели полностью прозрачны для клиентских компьютеров и серверов локальной сети, входящей в такую вирту-

альную сеть. Программное обеспечение этих узлов остается без изменений. Однако данный вариант характеризуется сравнительно низкой безопасностью информационного взаимодействия, поскольку частично трафик проходит по открытым каналам связи в незащищенном виде. Если создание и эксплуатацию такой VPN берет на себя провайдер ISP, тогда вся виртуальная частная сеть может быть построена на его шлюзах прозрачно для локальных сетей и удаленных пользователей предприятия. Но в этом случае возникают проблемы доверия к провайдеру и постоянной оплаты его услуг.

Защищенный туннель создается компонентами виртуальной сети, функционирующими на узлах, между которыми формируется туннель. Эти компоненты принято называть инициатором туннеля и терминатором туннеля.

Инициатор туннеля инкапсулирует исходный пакет в новый пакет, содержащий новый заголовок с информацией об отправителе и получателе. Инкапсулируемые пакеты могут принадлежать к протоколу любого типа, включая пакеты немаршрутизируемых протоколов, например NetBEUI. Все передаваемые по туннелю пакеты являются пакетами IP. Маршрут между инициатором и терминатором туннеля определяет обычная маршрутизируемая сеть IP, которая может быть сетью, отличной от Интернета.

Инициировать и разрывать туннель могут различные сетевые устройства и программное обеспечение. Например, туннель может быть инициирован ноутбуком мобильного пользователя, оборудованным модемом и соответствующим программным обеспечением для установления соединений удаленного доступа. В качестве инициатора может выступить также маршрутизатор локальной сети, наделенный соответствующей функциональностью. Туннель обычно завершается коммутатором сети или шлюзом провайдера услуг.

Терминатор туннеля выполняет процесс, обратный инкапсуляции. Терминатор удаляет новые заголовки и направляет каждый исходный пакет адресату в локальной сети.

Конфиденциальность инкапсулируемых пакетов обеспечивается путем их шифрования, а целостность и подлинность — путем формирования электронной цифровой подписи. Существует множество методов и алгоритмов криптографической защиты данных, поэтому необходимо, чтобы инициатор и терминатор туннеля своевременно согласовали друг с другом и использовали одни и те же методы и алгоритмы защиты. Для обеспечения возможности расшифрования данных и проверки цифровой подписи при приеме инициатор и терминатор туннеля должны также поддерживать функции безопасного обмена ключами. Кроме того, конечные стороны информационного взаимодействия должны пройти аутентификацию, чтобы гарантировать создание туннелей VPN только между уполномоченными пользователями.

Существующая сетевая инфраструктура корпорации может быть подготовлена к использованию VPN с помощью как программного, так и аппаратного обеспечения.

11.1.3. Средства обеспечения безопасности VPN

При построении защищенной виртуальной сети VPN первостепенное значение имеет задача обеспечения информационной безопасности. Согласно общепринятому определению под безопасностью данных понимают их конфиденциальность, целостность и доступность. Применительно к задачам VPN критерии безопасности данных могут быть определены следующим образом:

- *конфиденциальность* — гарантия того, что в процессе передачи данных по защищенным каналам VPN эти данные могут быть известны только легальным отправителю и получателю;
- *целостность* — гарантия сохранности передаваемых данных во время прохождения по защищенному каналу VPN. Любые попытки изменения, модификации, разрушения или создания новых данных будут обнаружены и станут известны легальным пользователям;
- *доступность* — гарантия того, что средства, выполняющие функции VPN, постоянно доступны легальным пользователям. Доступность средств VPN является комплексным показателем, который зависит от ряда факторов: надежности реализации, качества обслуживания и степени защищенности самого средства от внешних атак.

Конфиденциальность обеспечивается с помощью различных методов и алгоритмов симметричного и асимметричного шифрования. Целостность передаваемых данных обычно достигается с помощью различных вариантов технологии электронной подписи, основанных на асимметричных методах шифрования и односторонних функциях.

Аутентификация осуществляется на основе многоразовых и одноразовых паролей, цифровых сертификатов, смарт-карт, протоколов строгой аутентификации, обеспечивает установление VPN-соединения только между легальными пользователями и предотвращает доступ к средствам VPN нежелательных лиц.

Авторизация подразумевает предоставление абонентам, доказавшим свою легальность (аутентичность), разных видов обслуживания, в частности различных способов шифрования их трафика. Авторизация и управление доступом часто реализуются одними и теми же средствами.

Для обеспечения безопасности передаваемых данных в виртуальных защищенных сетях должны быть решены следующие основные задачи сетевой безопасности:

- взаимная аутентификация абонентов при установлении соединения;
- обеспечение конфиденциальности, целостности и аутентичности передаваемой информации;
- авторизация и управление доступом;
- безопасность периметра сети и обнаружение вторжений;
- управление безопасностью сети.

Аутентификация абонентов

Процедура аутентификации (установление подлинности) разрешает вход для легальных пользователей и предотвращает доступ к сети нежелательных лиц.

Современные средства идентификации и аутентификации должны удовлетворять двум условиям:

- поддерживать принцип единого входа в сеть;
- быть устойчивыми к сетевым угрозам (пассивному и активному прослушиванию сети).

Суть принципа единого входа в сеть состоит в том, что пользователь осуществляет один логический вход в сеть и после успешного прохождения аутентификации получает некоторый набор разрешений по доступу к сетевым ресурсам на все время работы в сети. Единый вход в сеть — это в первую очередь требование удобства для пользователей.

Второе требование можно реализовать, используя криптографические методы. В настоящее время общепринятыми являются подходы, основанные на службе каталогов с сертификатами в стандарте X.509 или системе Kerberos.

Процедуре аутентификации могут подвергаться не только пользователи, но и различные приложения, устройства и данные.

Методы, алгоритмы и ряд протоколов аутентификации подробно рассмотрены в главе 5; протоколы и системы аутентификации удаленных пользователей приведены в главе 12.

Обеспечение конфиденциальности, целостности и аутентичности информации

Задача обеспечения конфиденциальности информации заключается в защите передаваемых данных от несанкционированного чтения и копирования. Основным средством обеспечения конфиденциальности информации является шифрование.

Хотя главной заботой безопасности для компаний являются угрозы перехвата и просмотра данных в разделяемой сети, обеспечение целостности данных также является серьезной проблемой. Задача обеспечения целостности передаваемых данных заключается в проверке того, что данные в процессе передачи не были искажены злоумышленником или из-за ошибок передачи в сети. Аутентификация данных означает доказательство целостности этих данных, а также того, что они поступили от конкретного человека, который объявил об этом. Для осуществления аутентификации данных обычно используется криптографический механизм электронной цифровой подписи.

Необходимо обратить внимание на то, что у компьютерной криптографии две стороны — собственно криптографическая и интерфейсная, позволяющая сопрягаться с другими частями информационной системы. Стандартизация интерфейсов и их функциональное разнообразие

позволяют разрабатывать криптографические компоненты, которые можно было бы встраивать в существующие и перспективные конфигурации VPN. Алгоритмы шифрования и электронной цифровой подписи рассмотрены в главе 4.

Авторизация и управление доступом

Ключевым компонентом безопасности VPN является гарантия того, что доступ к компьютерным ресурсам получают авторизованные пользователи, в то время как для неавторизованных пользователей сеть полностью закрыта. Система авторизации имеет дело с легальными пользователями, которые успешно прошли процедуру аутентификации. Цель системы авторизации заключается в том, чтобы предоставить конкретному легальному пользователю те виды доступа к сетевым ресурсам, которые были определены для него администратором системы.

Система авторизации предоставляет легальным пользователям не только определенные права доступа к каталогам, файлам и принтерам, но и регулирует доступ пользователя к средствам шифрования пакетов, формирования цифровой подписи и определенным VPN-устройствам.

Процедуры авторизации реализуются программными средствами, встроенными в операционную систему или в приложение. При построении программных средств авторизации применяется два подхода:

- централизованная схема авторизации;
- децентрализованная схема авторизации.

Основное назначение централизованной системы авторизации — реализовать принцип единого входа. Управление процессом предоставления ресурсов пользователю осуществляется сервером. Централизованный подход к процессу авторизации реализован в системах Kerberos, RADIUS и TACACS.

При децентрализованном подходе к процессу авторизации каждая рабочая станция оснащается средствами защиты. В этом случае доступ к каждому приложению должен контролироваться средствами защиты той операционной среды, в которой работает данное приложение. Администратор сети должен контролировать работу средств безопасности, используемых всеми типами приложений. При удалении или добавлении новых пользователей администратору приходится конфигурировать доступ к каждой программе или системе.

В крупных сетях обычно применяется комбинированный подход в предоставлении легальным пользователям прав доступа к сетевым ресурсам. Сервер удаленного доступа ограничивает доступ пользователей к укрупненным элементам сети — подсетям, сегментам сети или корпоративным серверам. Каждый отдельный сервер сети осуществляет ограничение доступа пользователя к своим внутренним ресурсам — каталогам, приложениям или принтерам.

В последнее время активно развивается так называемое *ролевое управление доступом*. Оно не столько решает проблемы безопасности,

сколько улучшает управляемость систем. Суть ролевого управления доступом заключается в том, что между пользователями и их привилегиями помещают промежуточные сущности — роли. Для каждого пользователя одновременно могут быть активными несколько ролей, каждая из которых дает ему вполне определенные права.

Сложность информационной системы характеризуется прежде всего числом имеющихся в ней связей. Поскольку ролей намного меньше, чем пользователей и привилегий, использование ролей способствует понижению сложности и, следовательно, улучшению управляемости системы.

Кроме того, на основании ролевой модели управления доступом можно реализовать такой важный принцип, как разделение обязанностей (например, невозможность в одиночку скомпрометировать критически важный процесс). Между ролями могут быть определены статические или динамические отношения несовместимости (например, невозможность одному субъекту одновременно исполнять две роли).

Управление доступом и организация защищенного удаленного доступа рассматриваются в главах 5 и 12.

Безопасность периметра сети и обнаружение вторжений

Жесткий контроль доступа к приложениям, сервисам и ресурсам защищаемой сети является важной функцией правильно построенной сети. Использование таких средств безопасности, как межсетевые экраны, системы обнаружения вторжений, системы аудита безопасности, антивирусные комплексы, обеспечивает системную защиту перемещаемых по сети данных.

Важной частью общего решения безопасности сети являются межсетевые экраны, которые контролируют трафик, пересекающий периметр защищаемой сети, и накладывают ограничения на пропуск трафика в соответствии с политикой безопасности организации (см. главу 3). Межсетевые экраны защищают корпоративные сети от несанкционированного доступа к вычислительным ресурсам и от таких сетевых атак, как отказ в обслуживании. Несмотря на то что межсетевые экраны разрешают или запрещают прохождение трафика на основе таких критериев, как данные об источнике, пункте назначения, порте и др., они фактически не анализируют трафик.

Дополнительным элементом гарантии безопасности периметра сети является система предотвращения вторжений IPS (Intrusion Prevention System), работающая в реальном времени и предназначенная для обнаружения, фиксации и прекращения неавторизованной сетевой активности как от внешних, так и от внутренних источников.

Межсетевое экранирование и предотвращение вторжений предоставляют надежные механизмы защиты от сетевых атак.

Системы предотвращения вторжений рассматриваются в главе 13, системы защиты от вредоносных программ и спама описаны в главе 14.

Управление безопасностью сети

Сети VPN интегрируют как сами сетевые устройства, так и многочисленные сервисы управления безопасностью и пропускной способностью. Компаниям необходимо целостное управление этими устройствами и сервисами через инфраструктуру VPN, включая пользователей удаленного доступа и средств экстранет. В связи с этим управление средствами VPN становится одной из важнейших задач обеспечения эффективного функционирования VPN. Система управления корпоративной сетью должна включать необходимый набор средств для управления политиками безопасности, устройствами и сервисами VPN любого масштаба.

VPN дают возможность компаниям определить, какой уровень управления сетью им следует сохранить за собой, а какие функции целесообразно передать сервис-провайдерам. Многие компании предпочитают осуществлять полный контроль над развертыванием и функционированием своих VPN и, соответственно, хотят иметь всеобъемлющую систему управления сетью, основанную на политике безопасности компании.

Ключевыми компонентами управления являются политика безопасности, конфигурирование и мониторинг защищенной корпоративной сети. Для управления политикой безопасности и конфигурированием необходим набор средств управления, которые позволяют сформировать политику безопасности сети в соответствии с концепцией безопасности компании и обеспечить управление масштабируемым развертыванием и функционированием межсетевых экранов, виртуальных защищенных туннелей, средств аутентификации и шифрования и др.

Система управления безопасностью сети является краеугольным камнем семейства продуктов, обеспечивающих сквозную безопасность VPN. Для обеспечения высокого уровня безопасности и управляемости VPN, и в частности системы распределения криптографических ключей и сертификатов, необходимо обеспечить централизованное скоординированное управление безопасностью всей защищаемой корпоративной сети.

Методы и средства управления сетевой безопасностью рассматриваются в главе 15.

11.2. VPN-решения для построения защищенных сетей

В настоящее время технологии виртуальных защищенных частных сетей (VPN) привлекают внимание как средних, так и крупных компаний (банков, ведомств, крупных государственных структур и т. д.). Причина такого интереса заключается в том, что VPN-технологии действительно позволяют компаниям не только существенно сократить свои расходы на содержание выделенных каналов связи с удаленными

подразделениями (филиалами), но и повысить конфиденциальность обмена информацией.

VPN-технологии позволяют организовывать защищенные туннели как между офисами компании, так и к отдельным рабочим станциям и серверам. При этом неважно, через какого провайдера Интернета конкретная рабочая станция подключится к защищенным ресурсам предприятия. Все, что увидит сторонний наблюдатель, — поток IP-пакетов с нераспознаваемым содержимым [7, 68].

Рынок VPN-продуктов предлагает потенциальным клиентам широкий спектр оборудования и ПО для создания виртуальных защищенных сетей: от интегрированных многофункциональных и специализированных устройств до чисто программных продуктов.

11.2.1. Классификация сетей VPN

На смену традиционному способу установления соединений между пользователями Интернета посредством модемов и/или выделенных линий пришли виртуальные частные сети VPN, позволяющие пользователям свободно общаться между собой через Интернет [63]. На базе открытой для всех глобальной сети Интернет можно уверенно поддерживать практически все виды трафика, включая обмен данными, речь и видеоизображение. Благодаря преимуществам технологии VPN многие компании строят свою стратегию с учетом использования Интернета в качестве главного средства передачи информации, причем даже той, которая является уязвимой или жизненно важной.

Существуют разные варианты классификации VPN. Наиболее часто используют следующие три признака классификации:

- рабочий уровень модели OSI;
- архитектура технического решения VPN;
- способ технической реализации VPN.

Классификация VPN по рабочему уровню модели OSI

Для технологий безопасной передачи данных по общедоступной (незащищенной) сети применяют обобщенное название — *защищенный канал (Secure Channel)*. Термин «канал» подчеркивает тот факт, что защита данных обеспечивается между двумя узлами сети (хостами или шлюзами) вдоль некоторого виртуального пути, проложенного в сети с коммутацией пакетов.

Защищенный канал можно построить с помощью системных средств, реализованных на разных уровнях модели взаимодействия открытых систем OSI (рис. 11.5).

Классификация VPN по рабочему уровню модели OSI представляет значительный интерес, поскольку от выбранного уровня OSI во многом зависит функциональность реализуемой VPN и ее совместимость с

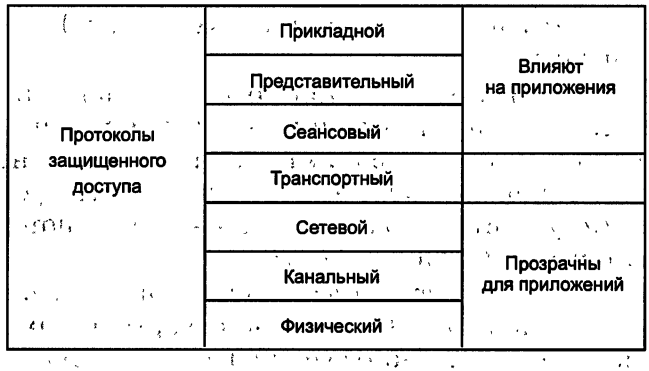


Рис. 11.5. Уровни протоколов защищенного канала

приложениями корпоративной информационной системы, а также с другими средствами защиты.

По признаку рабочего уровня модели OSI различают следующие группы VPN:

- VPN канального уровня;
- VPN сетевого уровня;
- VPN сеансового уровня.

Читатель, вероятно, заметил, что VPN строятся на достаточно низких уровнях модели OSI. Причина этого достаточно проста — чем ниже в стеке реализованы средства защищенного канала, тем проще их сделать прозрачными для приложений и прикладных протоколов. На сетевом и канальном уровнях зависимость приложений от протоколов защиты исчезает совсем. Поэтому построить универсальную и прозрачную защиту для пользователя возможно только на нижних уровнях модели. Однако здесь возникает другая проблема — зависимость протокола защиты от конкретной сетевой технологии.

Если для защиты данных используется протокол одного из верхних уровней (прикладного или представительного), то такой способ защиты не зависит от того, какие сети (IP или IPX, Ethernet или ATM) применяются для транспортировки данных, что можно считать несомненным достоинством. С другой стороны, приложение при этом становится зависимым от конкретного протокола защиты, т. е. для приложений такой протокол не является прозрачным.

Защищенному каналу на самом высоком, прикладном уровне свойствен еще один недостаток — ограниченная область действия. Протокол защищает только вполне определенную сетевую службу — файловую, гипертекстовую или почтовую. Например, протокол S/MIME защищает исключительно сообщения электронной почты. Поэтому для каждой службы необходимо разрабатывать соответствующую защищенную версию протокола. Следует отметить, что на верхних уровнях модели OSI существует достаточно жесткая связь между используемым стеком протоколов и приложением.

Рассмотрим более подробно группы VPN, работающие на канальном, сетевом и сеансовом уровнях модели OSI.

VPN канального уровня. Средства VPN, используемые на канальном уровне модели OSI, позволяют обеспечить инкапсуляцию различных видов трафика третьего уровня (и более высоких уровней) и построение виртуальных туннелей типа точка—точка (от маршрутизатора к маршрутизатору или от персонального компьютера к шлюзу ЛВС). К этой группе относятся VPN-продукты, которые используют протоколы L2F (Layer 2 Forwarding) и PPTP (Point-to-Point Tunneling Protocol), а также стандарт L2TP (Layer 2 Tunneling Protocol), разработанный совместно фирмами Cisco Systems и «Майкрософт».

Протокол защищенного канала PPTP основан на протоколе PPP, который широко используется в соединениях точка—точка, например при работе по выделенным линиям. Протокол PPTP обеспечивает прозрачность средств защиты для приложений и служб прикладного уровня и не зависит от применяемого протокола сетевого уровня. В частности, протокол PPTP может переносить пакеты как в сетях IP, так и в работающих на основе протоколов IPX, DECnet или NetBEUI. Однако, поскольку протокол PPP используется далеко не во всех сетях (в большинстве локальных сетей на канальном уровне работает протокол Ethernet, а в глобальных — протоколы ATM, Frame Relay), то PPTP нельзя считать универсальным средством. В разных частях крупной составной сети, вообще говоря, используются различные канальные протоколы, поэтому проложить защищенный канал через эту гетерогенную среду с помощью единого протокола канального уровня невозможно.

VPN сетевого уровня. VPN-продукты сетевого уровня выполняют инкапсуляцию IP в IP. Одним из широко известных протоколов на этом уровне является протокол IPSec (IP Security), предназначенный для аутентификации, туннелирования и шифрования IP-пакетов. Стандартизованный консорциумом Internet Engineering Task Force (IETF) протокол IPSec вобрал в себя все лучшие решения по шифрованию пакетов.

Работающий на сетевом уровне протокол IPSec является компромиссным вариантом. С одной стороны, он прозрачен для приложений, а с другой — он может работать практически во всех сетях, так как основан на широко распространенном протоколе IP. Протокол IPSec предусматривает стандартные методы идентификации пользователей или компьютеров при инициации туннеля, стандартные способы использования шифрования конечными точками туннеля, а также стандартные методы обмена и управления ключами шифрования между конечными точками.

Протокол IPSec является доминирующим методом VPN для взаимодействия ЛВС. Протокол IPSec может работать совместно с протоколом L2TP, в результате эти два протокола обеспечивают надежную идентификацию, стандартизованное шифрование и целостность данных. Туннель IPSec между двумя локальными сетями может поддерживать множество индивидуальных каналов передачи данных, в результате чего приложения данного типа получают преимущества с точки зрения масштабирования по сравнению с технологией второго уровня.

С протоколом IPSec связан протокол IKE (Internet Key Exchange), решающий задачи безопасного управления и обмена криптографическими ключами между удаленными устройствами. Протокол IKE автоматизирует обмен ключами и устанавливает защищенное соединение, тогда как IPSec кодирует и «подписывает» пакеты. Кроме того, IKE позволяет изменять ключ для уже установленного соединения, что повышает конфиденциальность передаваемой информации.

VPN сеансового уровня. Некоторые VPN используют другой подход под названием «посредники каналов» (Circuit Proxy). Этот метод функционирует над транспортным уровнем и ретранслирует трафик из защищенной сети в общедоступную сеть Интернет для каждого сокета в отдельности. (Сокет IP идентифицируется комбинацией TCP-соединения и конкретного порта или заданным портом UDP. Стек TCP/IP не имеет пятого — сеансового — уровня, однако ориентированные на сокеты операции часто называют операциями сеансового уровня.)

Шифрование информации, передаваемой между инициатором и терминатором туннеля, часто осуществляется с помощью защиты транспортного уровня TLS (Transport Layer Security). Для стандартизации аутентифицированного прохода через межсетевые экраны консорциум IETF определил протокол под названием SOCKS, и в настоящее время протокол SOCKS v.5 применяется для стандартизованной реализации посредников каналов.

Если протокол IPSec, по существу, распространяет сеть IP на защищенный туннель, то продукты на базе протокола SOCKS расширяют ее на каждое приложение и каждый сокет в отдельности. В отличие от решений уровня 3 (и уровня 2), где созданные туннели второго и третьего уровней функционируют одинаково в обоих направлениях, сети VPN уровня 5 допускают независимое управление передачей в каждом направлении. Аналогично протоколу IPSec и протоколам второго уровня, сети VPN уровня 5 можно использовать с другими типами виртуальных частных сетей, поскольку данные технологии не являются взаимоисключающими.

Классификация VPN по архитектуре технического решения

По архитектуре технического решения принято выделять три основных вида виртуальных частных сетей:

- внутрикорпоративные VPN;
- VPN с удаленным доступом;
- межкорпоративные VPN.

Внутрикорпоративные сети VPN (Intranet VPN) предназначены для обеспечения защищенного взаимодействия между подразделениями внутри предприятия или между группой предприятий, объединенных корпоративными сетями связи, включая выделенные линии.

Виртуальные частные сети VPN с удаленным доступом (Remote Access VPN) предназначены для обеспечения защищенного удаленного досту-

па к корпоративным информационным ресурсам мобильным и/или удаленным сотрудникам компании.

Межкорпоративные сети VPN (Extranet VPN) предназначены для обеспечения защищенного обмена информацией со стратегическими партнерами по бизнесу, поставщиками, крупными заказчиками, пользователями, клиентами и т. д. Экстранет-VPN обеспечивает прямой доступ из сети одной компании к сети другой компании и тем самым способствует повышению надежности связи, поддерживаемой в ходе делового сотрудничества.

Следует отметить, что в последнее время наблюдается тенденция к конвергенции различных конфигураций VPN.

Классификация VPN по способу технической реализации

Конфигурация и характеристики виртуальной частной сети во многом определяются типом применяемых VPN-устройств.

По способу технической реализации различают следующие группы VPN:

- VPN на основе маршрутизаторов;
- VPN на основе межсетевых экранов;
- VPN на основе программных решений;
- VPN на основе специализированных аппаратных средств со встроенными шифропроцессорами.

VPN на основе маршрутизаторов. Данный способ построения VPN предполагает применение маршрутизаторов для создания защищенных каналов. Поскольку вся информация, исходящая из локальной сети, проходит через маршрутизатор, то вполне естественно возложить на него и задачи шифрования. Пример оборудования для VPN на маршрутизаторах — устройства компании Cisco Systems.

VPN на основе межсетевых экранов. Межсетевые экраны большинства производителей поддерживают функции туннелирования и шифрования данных. В качестве примера решения на основе межсетевых экранов можно назвать продукт FireWall-1 компании Check Point Software Technologies. При использовании межсетевых экранов на базе ПК надо помнить, что подобное решение подходит для небольших сетей. Недостатками этого метода являются высокая стоимость решения в пересчете на одно рабочее место и зависимость производительности от аппаратного обеспечения, на котором работает межсетевой экран.

VPN на основе программного обеспечения. VPN-продукты, реализованные программным способом, с точки зрения производительности уступают специализированным устройствам, однако обладают достаточной мощностью для реализации VPN-сетей. Следует отметить, что в случае удаленного доступа требования к необходимой полосе пропускания невелики. Поэтому чисто программные продукты легко обеспечивают производительность, достаточную для удаленного доступа. Несомненным достоинством программных продуктов является гибкость и удобство в применении, а также относительно невысокая стоимость.

VPN на основе специализированных аппаратных средств. Главным преимуществом VPN на основе специализированных аппаратных средств является их высокая производительность. Более высокое быстродействие специализированных VPN-систем обусловлено тем, что шифрование в них осуществляется специализированными микросхемами. Специализированные VPN-устройства обеспечивают высокий уровень безопасности, однако обладают высокой стоимостью.

11.2.2. Основные варианты архитектуры VPN

Существует множество разновидностей виртуальных частных сетей. Их спектр варьируется от провайдерских сетей, позволяющих управлять обслуживанием клиентов непосредственно на их площадях, до корпоративных сетей VPN, разворачиваемых и управляемых самими компаниями. Однако принято выделять три основных вида виртуальных частных сетей: VPN с удаленным доступом, внутрикорпоративные VPN и межкорпоративные VPN [7].

VPN с удаленным доступом

Виртуальные частные сети VPN с удаленным доступом обеспечивают защищенный удаленный доступ к информационным ресурсам предприятия для мобильных или удаленных сотрудников корпорации (руководства компании, сотрудников, находящихся в командировках, сотрудников-надомников и т. д.).

Виртуальные частные сети с удаленным доступом (рис. 11.6) завоевали всеобщее признание благодаря тому, что они позволяют значительно сократить ежемесячные расходы на использование коммутируемых и выделенных линий. Принцип их работы прост: пользователи ус-

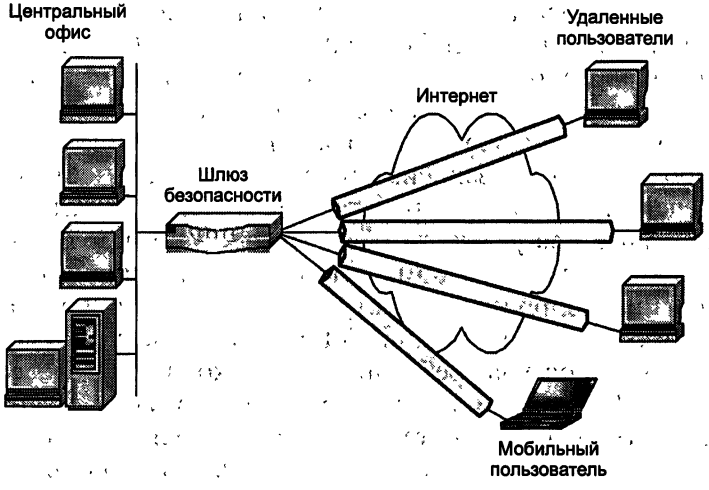


Рис. 11.6. Виртуальная частная сеть с удаленным доступом

танавливают соединения с местной точкой доступа к глобальной сети, после чего их вызовы туннелируются через Интернет, что позволяет избежать платы за междугородную и международную связь или выставления счетов владельцам бесплатных междугородных номеров. Затем все вызовы концентрируются на соответствующих узлах и передаются в корпоративные сети.

Переход к VPN с удаленным доступом дает ряд преимуществ, в частности:

- эффективную систему установления подлинности удаленных и мобильных пользователей, которая обеспечивается надежной процедурой аутентификации;
- высокую масштабируемость и простоту развертывания для новых пользователей, добавляемых к сети;
- сосредоточение внимания компании на основных корпоративных бизнес-целях вместо отвлечения на проблемы обеспечения работы сети.

Существенная экономия при использовании VPN с удаленным доступом является мощным стимулом, однако применение открытого Интернета в качестве объединяющей магистрали для транспорта чувствительного корпоративного трафика становится все более масштабным, что делает механизмы защиты информации жизненно важными элементами данной технологии.

Внутрикорпоративная сеть VPN

Внутрикорпоративные сети VPN используются для организации защищенного взаимодействия между подразделениями внутри предприятия или между группой предприятий, объединенных корпоративными сетями связи. Компании, нуждающиеся в организации доступа к централизованным хранилищам информации для своих филиалов и отделений, могут соединить удаленные узлы при помощи виртуальной частной сети (рис. 11.7). Внутрикорпоративные сети VPN строятся с использованием Интернета или разделяемых сетевых инфраструктур, предоставляемых сервис-провайдерами. Компания может отказаться от использования дорогостоящих выделенных линий, заменив их более дешевой связью через Интернет. Это существенно сокращает расходы на использование полосы пропускания, поскольку в Интернете расстояние никак не влияет на стоимость соединения.

Для внутрикорпоративных сетей VPN характерны следующие достоинства:

- применение мощных криптографических протоколов шифрования данных для защиты конфиденциальной информации;
- надежность функционирования при выполнении таких критических приложений, как системы автоматизированной продажи и системы управления базами данных;

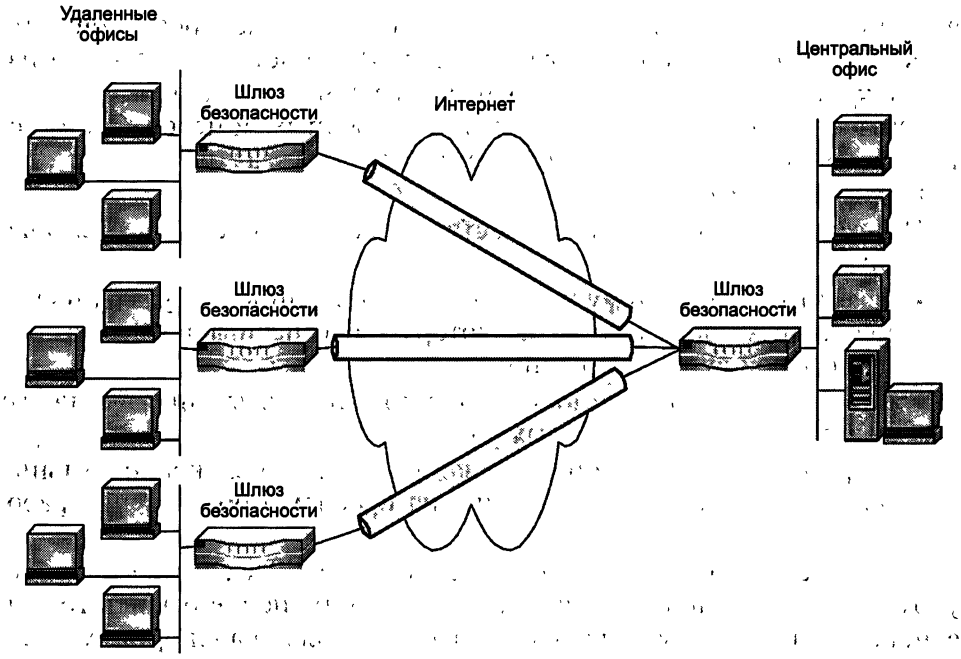


Рис. 11.7. Соединение узлов сети с помощью технологии внутрикорпоративных сетей VPN

- гибкость управления для более эффективного размещения быстро возрастающего количества новых пользователей, новых офисов и новых программных приложений.

Построение внутрикорпоративных сетей VPN, использующих Интернет, является самым рентабельным способом реализации VPN-технологии. Однако в Интернете уровни сервиса вообще не гарантируются. Компании, которым требуются гарантированные уровни сервиса, должны рассмотреть возможность развертывания своих VPN с использованием разделяемых сетевых инфраструктур, предоставляемых сервис-провайдерами.

Межкорпоративная сеть VPN

Межкорпоративные сети VPN используются для организации эффективного взаимодействия и защищенного обмена информацией со стратегическими партнерами по бизнесу, в том числе зарубежными, основными поставщиками, крупными заказчиками, клиентами и т. д. (рис. 11.8). Экстранет — это сетевая технология, которая обеспечивает прямой доступ из сети одной компании к сети другой компании и таким образом способствует повышению надежности связи, поддерживаемой в ходе делового сотрудничества.

Межкорпоративные сети VPN в целом похожи на внутрикорпоративные виртуальные частные сети с той лишь разницей, что проблема защиты информации является для них более острой. Для межкорпора-

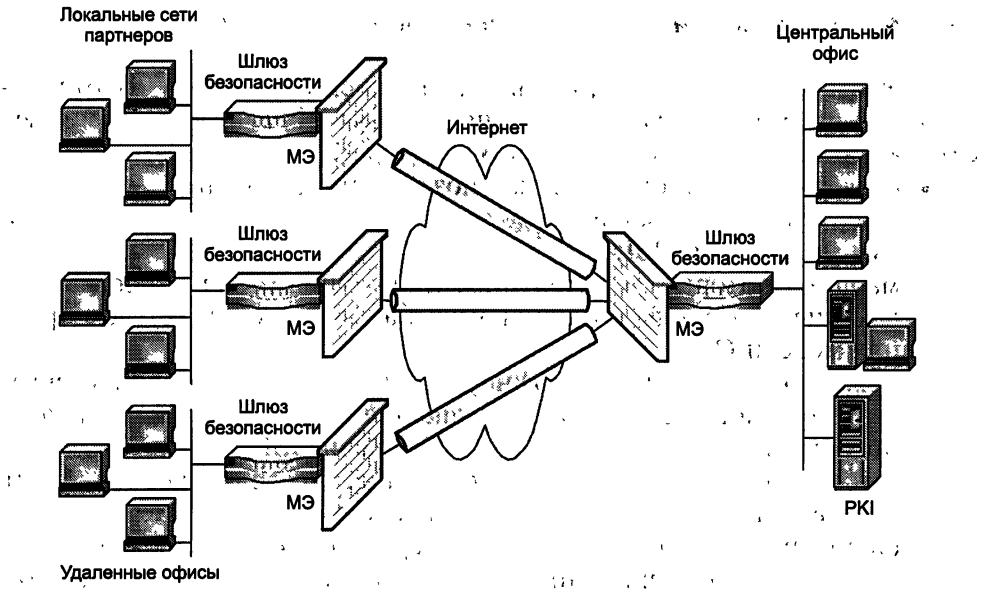


Рис. 11.8. Межкорпоративная сеть VPN

тивных сетей VPN характерно использование стандартизированных VPN-продуктов, гарантирующих способность к взаимодействию с различными VPN-решениями, которые деловые партнеры могли бы применять в своих сетях.

Когда несколько компаний принимают решение работать вместе и открывают друг для друга свои сети, они должны позаботиться о том, чтобы их новые партнеры имели доступ только к определенной информации. При этом конфиденциальная информация должна быть надежно защищена от несанкционированного использования. Именно поэтому в межкорпоративных сетях большое значение придается контролю доступа из открытой сети посредством межсетевых экранов. Важна и аутентификация пользователей, призванная гарантировать, что доступ к информации получают только те, кому он действительно разрешен. Вместе с тем развернутая система защиты от несанкционированного доступа не должна привлекать к себе внимания.

Соединения экстранет-VPN развертываются, используя те же самые архитектуру и протоколы, которые применяются при реализации интранет-VPN и VPN с удаленным доступом. Основное различие заключается в том, что разрешение доступа, которое дается пользователям экстранет-VPN, связано с сетью их партнера.

Иногда в отдельную группу выделяют локальный вариант сети VPN (Localnet VPN). Локальная сеть VPN обеспечивает защиту информационных потоков, циркулирующих внутри локальных сетей компании (как правило, центрального офиса) от несанкционированного доступа со стороны излишне любопытных сотрудников самой компании. В настоящее время наблюдается тенденция к конвергенции различных способов реализаций VPN [7, 68].

11.2.3. Основные виды технической реализации VPN

Средства построения виртуальных защищенных сетей VPN отличаются большим разнообразием. Для построения VPN могут применяться сетевые средства защиты следующих категорий:

- серверы удаленного доступа, позволяющие создавать защищенные туннели на канальном уровне эталонной модели сетевого взаимодействия OSI;
- маршрутизаторы со встроенными функциями VPN, поддерживающие протоколы создания VPN на канальном и сетевом уровнях модели OSI;
- межсетевые экраны, возможно, включающие в свой состав серверы удаленного доступа и позволяющие создавать VPN на канальном, сетевом и сеансовом уровнях модели OSI;
- автономное программное обеспечение, позволяющее создавать VPN в основном на сетевом и сеансовом уровнях модели OSI;
- специализированные аппаратные средства, ориентированные на формирование защищенных туннелей на канальном и сетевом уровнях модели OSI.

Средства построения VPN могут отличаться друг от друга по многим характеристикам: точкам размещения VPN-устройств; типу платформы, на которой эти средства работают; реализуемым протоколам формирования защищенных каналов; набору функций; применяемым алгоритмам шифрования и протоколам аутентификации.

Как отмечалось выше, по способу технической реализации различают следующие группы VPN:

- VPN на основе маршрутизаторов;
- VPN на основе межсетевых экранов;
- VPN на основе программных решений;
- VPN на основе специализированных аппаратных средств.

Каждое из перечисленных решений имеет свои достоинства и недостатки. Следует иметь в виду, что корпоративные заказчики предъявляют, как правило, достаточно жесткие требования к таким технико-экономическим характеристикам VPN, как:

- интегрируемость с уже существующими в подразделениях компании средствами защиты информации, а также прозрачность VPN для всех работающих внутрикорпоративных приложений (системы документооборота, системы аудита и управления компьютерными сетями и т. д.);
- масштабируемость применяемых технических решений;
- пропускная способность защищаемой сети, т. е. VPN-устройства не должны вносить существенные задержки в процесс обработки и передачи информации, а также заметно суживать полосу пропускания канала связи;
- стойкость применяемых криптоалгоритмов, которая надежно защищала бы корпоративную информацию от криптоаналитических атак злоумышленников и недобросовестных конкурентов, а

также обеспечение целостности передаваемой по сетям информации и надежной аутентификации пользователей VPN;
- унифицируемость VPN-решения, позволяющая данной компании в будущем без особых технических и организационных проблем устанавливать защищенные соединения с новыми партнерами по бизнесу;
- общая совокупная стоимость построения корпоративной VPN.

VPN на базе маршрутизаторов

Маршрутизатор пропускает через себя все пакеты, которыми локальная сеть обменивается с внешним миром. Это делает маршрутизатор естественной платформой для шифрования исходящих пакетов и расшифрования криптозащищенных входящих пакетов. Иными словами, маршрутизатор может, в принципе, совмещать основные операции по маршрутизации с поддержанием функций VPN.

Такое решение имеет свои достоинства и недостатки. Достоинства заключаются в удобстве совместного администрирования функций маршрутизации и VPN. Применение маршрутизаторов для поддержания VPN особенно полезно в тех случаях, когда предприятие не использует межсетевой экран и организует защиту корпоративной сети только с помощью маршрутизатора, совмещающего функции защиты как по доступу в сеть, так и по шифрованию передаваемого трафика. Недостатки данного решения связаны с повышенными требованиями к производительности маршрутизатора, вынужденного совмещать основные операции по маршрутизации с трудоемкими операциями шифрования и аутентификации трафика.

Проблема получения повышенной производительности маршрутизатора обычно решается с помощью аппаратной поддержки функций шифрования. Сегодня практически все ведущие производители маршрутизаторов и других сетевых устройств заявляют о поддержке в своих продуктах различных VPN-протоколов.

VPN на базе межсетевых экранов

Через межсетевой экран локальной сети, как и через маршрутизатор, пропускается весь трафик. Поэтому функции зашифрования исходящего трафика и расшифрования входящего трафика может с успехом выполнять и МЭ. Сегодня ряд VPN-решений опирается на расширения МЭ дополнительными функциями поддержки VPN, что позволяет установить через Интернет шифрованное соединение с другим МЭ.

Построение VPN на базе межсетевых экранов является вполне обоснованным решением с точки зрения обеспечения комплексной защиты корпоративной сети от атак из открытых сетей. Действительно, при объединении функций МЭ и VPN-шлюза в одной точке под контролем единой системы управления и аудита все функции по защите

корпоративной сети оказываются сосредоточенными в одном устройстве, при этом повышается качество администрирования средств защиты.

Однако такая универсализация средства защиты при существующем уровне возможностей вычислительных средств имеет не только положительные, но и отрицательные стороны. Вычислительная сложность у операций шифрования и аутентификации намного выше, чем у традиционных для межсетевого экрана операций фильтрации пакетов. Поэтому МЭ, рассчитанный на выполнение менее трудоемких операций, часто не обеспечивает нужную производительность при выполнении дополнительных функций VPN. Когда корпоративная сеть подключена к открытой сети через высокоскоростной канал, рекомендуется для обеспечения качественной защиты использовать VPN-шлюз, выполненный в виде отдельного аппаратного, программного или комбинированного устройства.

Ряд производителей МЭ расширяют поддержку функций VPN в своих продуктах. Ведущими производителями межсетевых экранов с поддержкой функций VPN являются компании Check Point Software Technologies, Network Associates, Secure Computing и др. В частности, компания Check Point Software Technologies, чей межсетевой экран FireWall-1 многократно признавался лучшим, выпускает популярное семейство продуктов VPN-1, которое тесно интегрировано с FireWall-1.

Большинство МЭ представляют собой серверное программное обеспечение, поэтому актуальная проблема повышения производительности может быть решена за счет применения высокопроизводительной компьютерной платформы. Построение VPN на базе МЭ выглядит вполне рациональным решением, хотя ему присущи некоторые недостатки. Прежде всего это значительная стоимость данного решения в пересчете на одно рабочее место корпоративной сети и достаточно высокие требования к производительности МЭ даже при умеренной ширине полосы пропускания выходного канала связи.

VPN на базе специализированного программного обеспечения

Для построения VPN широко используются специализированные программные средства. Программные средства построения VPN позволяют формировать защищенные туннели чисто программным образом и превращают компьютер, на котором они функционируют, в маршрутизатор TCP/IP, который получает зашифрованные пакеты, расшифровывает их и передает по локальной сети дальше, к конечной точке назначения. В последнее время появилось достаточно много таких продуктов. В виде специализированного программного обеспечения могут быть выполнены VPN-шлюзы, VPN-серверы и VPN-клиенты.

VPN-продукты, реализованные программным способом, с точки зрения производительности уступают специализированным аппаратным устройствам; в то же время программные продукты легко обеспечивают производительность, достаточную для удаленного доступа. Не-

сомненным достоинством программных продуктов являются гибкость и удобство в применении, а также относительно невысокая стоимость. Многие компании-производители аппаратных шлюзов дополняют линейку своих продуктов чисто программной реализацией VPN-клиента, который рассчитан на работу в среде стандартной ОС.

VPN на основе специализированных аппаратных средств

Главным преимуществом VPN-средств на основе специализированных аппаратных устройств является их высокая производительность. Объем вычислений, которые необходимо выполнить при обработке VPN-пакета, в 50—100 раз превышает тот, который требуется для обработки обычного пакета. Более высокое быстродействие VPN-систем на базе аппаратных средств достигается благодаря тому, что шифрование в них осуществляется специализированными микросхемами.

Такие VPN-средства чаще всего совместимы с протоколом IPSec и применяются для формирования криптозащищенных туннелей между локальными сетями. Оборудование для формирования VPN от некоторых производителей одновременно поддерживает и защищенную связь в режиме «удаленный компьютер—локальная сеть».

Аппаратные VPN-шлюзы реализуются в виде отдельного аппаратного устройства, основной функцией которого является высокопроизводительное шифрование трафика. Эти VPN-шлюзы работают с цифровыми сертификатами X.509 и инфраструктурой управления открытыми ключами PKI, поддерживают работу со справочными службами по LDAP.

Специализированные аппаратные VPN-средства лидируют практически по всем возможным показателям, кроме стоимости. Специализированное аппаратное VPN-оборудование является предпочтительным решением для ответственных применений.

11.3. Современные отечественные VPN-продукты

Продукты сетевой безопасности выпускают в настоящее время ряд российских компаний: ЛАН Крипто, ООО «Анкад», компания «С-Терра СиЭсПи», НИП «Информзащита», ОАО «ИнфоТеКС», ООО «Фактор-ТС» и др.

Сравнительный анализ продуктов сетевой безопасности российских производителей показал, что новая версия семейства VPN-продуктов CSP VPN 3.0 компании «С-Терра СиЭсПи» имеет высокие характеристики и отличается оптимизированной производительностью и повышенной устойчивостью при функционировании на многопроцессорных (многоядерных) платформах [101]. Рассмотрим семейство VPN-продуктов CSP VPN.

11.3.1. Семейство VPN-продуктов компании «С-Терра СиЭсПи»

CSP VPN-агенты российской компании «С-Терра СиЭсПи» являются частью решения по безопасности Cisco, адаптированного к российским стандартам информационной безопасности, и предназначены для использования в рамках идеологии CiscoSAFE. Реализована совместимость продуктов семейства CSP VPN Gate с системой централизованного управления Cisco Security Manager (CS Manager). Эта система обеспечивает централизованное управление политиками безопасности МЭ, VPN и IPS, масштабируемость, наследование политик, группирование устройств и визуальное управление политиками, ролевой механизм управления правами доступа и документооборот по операциям. В результате пользователи получают гибкий, надежный, прозрачный и эффективный инструмент централизованного управления всеми устройствами сети, включая продукты CSP VPN Gate.

Среди других нововведений и улучшений можно отметить модернизацию командной строки CLI IOS и поддержку ОС Windows Vista.

Функционально полный комплект средств сетевой защиты CSP VPN обеспечивает:

- защиту индивидуальных пользователей;
- защиту серверов;
- защиту отдельных сетей;
- защиту специализированных устройств.

Продуктная линия CSP VPN включает:

- *CSP VPN Client.* Программный продукт для защиты индивидуальных пользователей;
- *CSP VPN Server.* Программный продукт для сетевой защиты серверов;
- *CSP VPN Gate 100B.* Программно-аппаратный комплекс — шлюз безопасности, ориентированный на защиту специализированных устройств;
- *CSP VPN Gate 100.* Программно-аппаратный комплекс — шлюз безопасности, ориентированный на защиту малых офисов (до 10 компьютеров);
- *CSP VPN Gate 1000.* Программно-аппаратный комплекс — шлюз безопасности, ориентированный на защиту малых офисов (до 50 компьютеров);
- *CSP VPN Gate 3000.* Программно-аппаратный комплекс — шлюз безопасности, ориентированный на защиту средних офисов (до 250 компьютеров);
- *CSP VPN Gate 7000.* Программно-аппаратный комплекс — шлюз безопасности, ориентированный на защиту крупных офисов (свыше 250 компьютеров);
- *модуль NME-RVPN (Russia VPN Network Module).* Программно-аппаратный комплекс — шлюз безопасности, предназначенный для

использования в составе маршрутизаторов серии Cisco 2800 и 3800 Integrated Services Routers.

Рассмотрим подробнее характеристики и возможности программно-аппаратного шлюза безопасности — модуля NME-RVPN.

Модуль NME-RVPN

Модуль NME-RVPN в составе маршрутизаторов серии Cisco 2800 и 3800 Integrated Services Routers предлагает российским потребителям уникальное устройство, позволяющее обеспечить как эффективную маршрутизацию, так и защиту трафика данных, голоса, видео (рис. 11.9). При этом устройство управляется как единое целое, используя интерфейс Cisco для формирования правил маршрутизации и защиты сетевых взаимодействий. Подобная глубокая интеграция позволяет существенно уменьшить сложность сети, не предъявлять дополнительных требований к квалификации персонала и, как результат, снизить затраты на развертывание и поддержку, а также сроки развертывания подсистемы информационной безопасности.

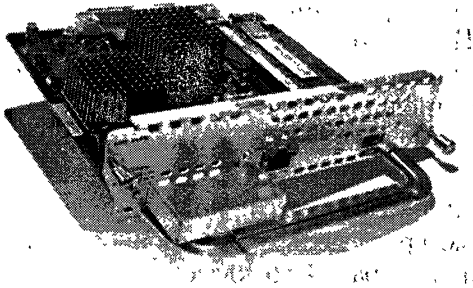


Рис. 11.9. Модуль NME-RVPN

Обеспечение защищенности сетевых взаимодействий

В связи с широкой интеграцией корпоративных коммуникаций с публичными сетями для обеспечения взаимодействий компаний с филиалами, удаленными пользователями, заказчиками и партнерами первостепенное значение приобретает вопрос обеспечения российских пользователей высокотехнологичным сертифицированным VPN-решением в сочетании с передовыми технологиями Cisco Systems, удовлетворяющим современным требованиям эффективной защиты всех видов сетевых взаимодействий.

При этом необходимо не только решить вопросы защиты внешнего обмена данными, но и предоставить современные решения по защищенным беспроводным коммуникациям, защите голоса и видео с обеспечением качества обслуживания, максимально эффективно защитить взаимодействие клиентов в сетях операторов связи и услуг.

Интеграция модуля NME-RVPN в маршрутизаторы серии Cisco 2800 или 3800 Integrated Services Router позволяет потребителям получить единое решение, которое обеспечивает в том числе организацию сетевой защиты, использующей российскую сертифицированную криптографию, развитую маршрутизацию, качество обслуживания приоритетного трафика (QoS), сервисы IP-телефонии и видео, коммутацию сетей. Подобные качества совместно с управляемостью и технологией Cisco IOS, практически полностью удовлетворяют потребность современного бизнеса в организации и защите ответственных, критически важных сетевых взаимодействий.

Программное обеспечение CSP VPN Gate

Программное обеспечение CSP VPN Gate, входящее в состав модуля NME-RVPN, является еще одним элементом семейства продуктов CSP VPN Client, CSP VPN Server и масштабируемой серии шлюзов безопасности CSP VPN Gate 100/1000/3000/7000/10000.

Продукты CSP VPN обеспечивают базовую функциональность современного VPN-устройства:

- шифрование (конфиденциальность) и ЭЦП (целостность, аутентификация) IP-пакетов, целостность потока пакетов;
- маскировку топологии сети за счет инкапсуляции трафика в защищенный туннель;
- прозрачность для NAT (поддержка инкапсуляции пакета ESP в UDP);
- аутентификацию узлов сети и пользователей, контроль доступа на уровне компьютеров, пользователей и приложений, интегрированный межсетевой экран 4-го класса (CSP VPN Gate удовлетворяет требованиям к межсетевому экрану по 4-му классу защищенности);
- обеспечение надежности с выравниванием нагрузки в схеме резервирования $N + 1$ (Dead Peer Detection Protocol);
- унификацию политики безопасности для мобильных и внутренних пользователей (динамическое конфигурирование корпоративных IP-адресов для удаленных пользователей внутри VPN);
- сохранение классификации трафика для защищенных пакетов, приоритетную обработку трафика голоса и видео (поддержка QoS), отсутствие потери пакетов при регенерации сессионных ключей (Smooth IKE Re-keying);
- гибкое, централизованное и событийное ведение журнала с возможностью вторичной обработки на основе протокола Syslog.

Как результат, применение модуля NME-RVPN в составе маршрутизатора Cisco Integrated Services Router 2800/3800 обеспечивает эффективную реализацию множества сценариев сертифицированной защиты, включая:

- межсетевые взаимодействия;
- защищенный доступ удаленных и мобильных пользователей;

- защиту беспроводных сетей;
- защиту мультисервисных сетей (включая IP-телефонию и видеоконференц-связь);
- защиту платежных систем и систем управления технологическими процессами в производстве и на транспорте.

Межсетевые взаимодействия

Сценарии защиты межсетевых взаимодействий (Site-to-Site VPN) применяются для защиты коммуникаций территориально распределенных корпоративных сетей через публичные (открытые, не заслуживающие доверия) сети/каналы связи.

По сути, применение VPN-решений для этих целей не должно приводить к понижению требований к характеристикам непосредственно канала передачи данных, таких как поддержка множественности протоколов, высокая надежность, большая масштабируемость. Наоборот, современные VPN-решения должны обеспечивать высокую ценовую эффективность и большую гибкость в реализации таких требований. Высокую ценовую эффективность можно получить, например, за счет возможности использовать публичные каналы для передачи информации, что ранее было недоступно. Использование для этой цели маршрутизаторов Cisco ISR (рис. 11.10) в полной мере выполняет поставленную выше задачу.

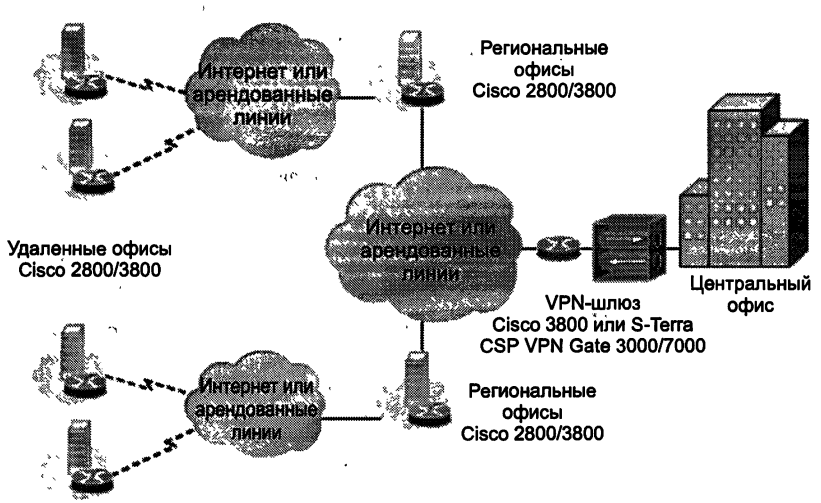


Рис. 11.10. Использование VPN-туннелей для создания защищенной корпоративной сети

Для выполнения требований повышенной надежности сетевых взаимодействий крупных сетей (обеспечивающей непрерывность бизнес-процессов в них) в дополнение к приведенному выше примеру могут использоваться решения с резервированием и балансировкой нагрузки.

Защита беспроводных и мультисервисных сетей

Продукты CSP VPN поддерживают сценарии защиты как выделенных мультимедийных, так и смешанных сетей, обеспечивая:

- поддержку качества сетевого обслуживания;
- защиту качества сервиса в голосовой VPN при перегрузке трафика данных.

Модуль NME-RVPN в составе маршрутизаторов Cisco 2800 или Cisco 3800, обеспечивающих дополнительную функциональность Cisco Unified CallManager Express и беспроводной точки доступа, предоставляет для удаленных офисов все необходимые возможности обработки и защиты беспроводных мультимедийных и мультисервисных сетей в едином устройстве.

Основным средством защиты трафика в беспроводной сети является IPsec. При этом обеспечивается не только аутентификация устройств (что делается на канальном уровне), но и аутентификация пользователей (рис. 11.11). Применение в радиосегменте выделенного адресного пространства и IPsec VPN обеспечивает возможность:

- изолировать проводной сегмент от открытого IP-трафика;
- пропускать внутрь проводной корпоративной сети (к ресурсам локальной сети) только IPsec-трафик, причем только в «домашние» сети.

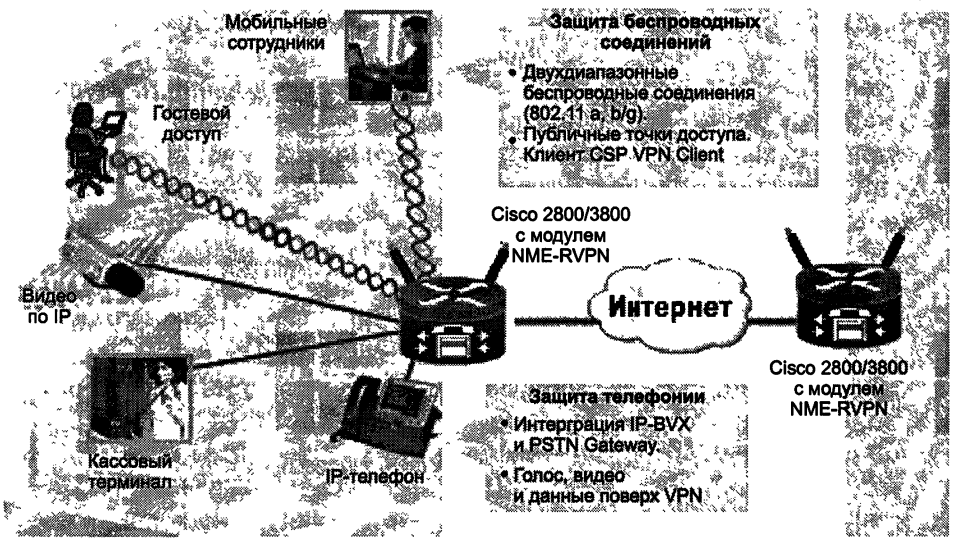


Рис. 11.11. Защита беспроводных и мультисервисных сетей

Защита удаленных и мобильных пользователей

Сценарии удаленного доступа пользователей применяются для защиты доступа удаленных или мобильных пользователей в корпоратив-

ную сеть через публичные (открытые, не заслуживающие доверия) сети или каналы связи:

- политика безопасности клиента доступа CSP VPN Client определяется только системным администратором (администратором безопасности) и не может быть изменена пользователем;
- права доступа пользователя определяются в корпоративной сети, и информация о правах доступа в корпоративной сети отсутствует на клиенте доступа CSP VPN Client;
- клиент доступа CSP VPN Client не требует от пользователя никаких технических операций, кроме установки и ввода ключа, предоставленного администратором безопасности.

CSP VPN Client поддерживает защищенную связь практически из любой точки, где присутствует какой-либо коммуникационный ресурс. Используются специальные меры в обеспечении мобильности пользователя:

- адаптивность к адресному пространству (IPsec автоматически включается в зонах, где требуется защищенное соединение);
- поддержка различных сред передачи, в том числе мобильных (GPRS, CDMA, Wi-Fi, WiMAX и др.);
- обеспечение прозрачной передачи IKE/IPsec-трафика через шлюзы с трансляцией адресов (NAT).

Возможности и преимущества модуля NME-RVPN

По сравнению с другими отдельными подобными устройствами модуль NME-RVPN при использовании в сетевой инфраструктуре центрального офиса имеет ряд преимуществ:

- общий с другими устройствами интерфейс управления. Для управления и конфигурирования модуля можно применять интерфейс командной строки (CLI) с использованием команд, аналогичных Cisco IOS. Модулем можно также управлять с помощью графического веб-интерфейса;
- снижение потребления и простота коммутации. Модуль получает питание от маршрутизатора, не нуждается в коммутации и не занимает места в стойке с сетевым оборудованием.

Архитектура модуля NME-RVPN

Модуль NME-RVPN можно установить в маршрутизаторы Cisco ISR 2811, 2821, 2851, 3825 и 3845 с версией IOS 12.4(11)T или выше. Модуль может работать с любым образом (Feature Set) IOS, начиная с IP base. При этом модуль NME-RVPN работает независимо от IOS-маршрутизатора, используя программное обеспечение CSP VPN Gate v 2.1 компании «С-Терра СиЭсПи», установленное на компакт-флэш-карте (Compact Flash) модуля. Программное обеспечение модуля функционирует под управлением адаптированной ОС Linux.

Аппаратно модуль NME-RVPN представляет собой вычислительную платформу на базе процессора Intel Celeron-M 1,0 ГГц с оперативной памятью 512 Мб и компакт-флэш-картой 512 Мб. Для подключения к локальной сети модуль имеет внешний интерфейс Gigabit Ethernet. Аналогичный внутренний интерфейс осуществляет взаимодействие и передачу данных между модулем и маршрутизатором.

Производительность

Наиболее часто используемый алгоритм для IPsec-туннелей, включающий шифрование с проверкой целостности (ESP+HMAC), показывает производительность, равную 40 Мбит/с (измерено на больших пакетах — 1400 байт). Если же проверка целостности неважна, то в режиме **ESP only** модуль может обеспечить скорость шифрования до 95 Мбит/с.

Вопросы для самоконтроля

1. Что такое виртуальные защищенные сети VPN?
2. Сформулируйте концепцию построения виртуальных защищенных сетей VPN.
3. Объясните следующие понятия: виртуальный защищенный туннель, туннелирование и инкапсуляция.
4. Дайте развернутые определения таких устройств, как VPN-клиент, VPN-сервер и VPN-шлюз безопасности.
5. Поясните особенности структуры и функционирования двух основных схем виртуальных защищенных каналов.
6. Каковы функции инициатора туннеля и терминатора туннеля?
7. Какие методы используют для обеспечения безопасности сетей VPN?
8. Приведите классификацию сетей VPN по рабочему уровню модели взаимодействия открытых систем OSI.
9. Каковы основные варианты архитектуры сетей VPN? Дайте пояснение для каждого из трех основных вариантов.
10. Укажите основные виды технической реализации VPN и дайте пояснения для каждого из них.
11. Какие российские компании выпускают VPN-продукты в настоящее время?
12. Опишите возможности и основные характеристики семейства VPN-продуктов CSP VPN 3.0 российской компании «С-Терра СиЭсПи».

Глава 12
ЗАЩИТА УДАЛЕННОГО ДОСТУПА

Развитие информационных технологий позволяет повысить эффективность деятельности компаний, а также открывает новые возможности для взаимодействия с потенциальными клиентами на базе общедоступных сетей, в том числе Интернета. Создание веб-сайта — своеобразного представительства предприятия в Интернете — является лишь первым шагом на этом пути. Активное ведение коммерческих операций в Сети предполагает массовый доступ потребителей электронных услуг (или веб-клиентов) к интернет-приложениям и проведение электронных транзакций миллионами пользователей Сети. Размещение интернет-приложений внутри корпоративной сети может нанести ущерб безопасности ИТ-инфраструктуры, поскольку открытие доступа через межсетевой экран неизбежно создает потенциальную возможность для несанкционированного проникновения злоумышленников в сеть предприятия.

Обеспечение информационной безопасности должно включать решение таких задач, как безопасный доступ к веб-серверам и веб-приложениям, аутентификация и авторизация пользователей, обеспечение целостности и конфиденциальности данных и др.

Сегодня организации нуждаются в надежных, гибких и безопасных методах и средствах для получения и использования открытой и конфиденциальной информации многочисленными группами людей — своими сотрудниками, партнерами, клиентами и поставщиками. Проблема заключается в том, чтобы обеспечить доступ к такой информации только авторизованным пользователям. Целесообразно применять интегрированную систему управления доступом пользователей к чувствительной информации в широком диапазоне точек доступа и приложений. Такая система решает многие проблемы контроля доступа, с которыми сталкиваются организации, обеспечивая при этом удобный доступ и высокую безопасность.

12.1. Особенности удаленного доступа

Для реализации растущих потребностей электронного бизнеса необходимо построить надежную с точки зрения безопасности среду для осуществления различных операций в онлайновом режиме. Техноло-

гии, которые дают возможность осуществлять электронный бизнес, выполняют четыре основные функции:

- аутентификацию, или проверку подлинности пользователя;
- управление доступом, позволяющее авторизованным пользователям получать доступ к требуемым ресурсам;
- шифрование, гарантирующее, что связь между пользователем и базовой инфраструктурой защищена;
- неотказуемость, означающую, что пользователи не могут позднее отказаться от выполненной транзакции (обычно реализуется с помощью цифровой подписи и инфраструктуры открытых ключей) — рис. 12.1.

Рис. 12.1. Технологии, обеспечивающие электронный бизнес

Только решение, которое выполняет все четыре эти функции, может создать доверенную среду, способную по-настоящему обеспечить реализацию электронного бизнеса.

Управление доступом является критическим компонентом общей системы безопасности. Система управления доступом обеспечивает авторизованным пользователям доступ к надлежащим ресурсам. Проектирование этой инфраструктуры требует тонкого баланса между предоставлением доступа к критическим ресурсам только авторизованным пользователям и обеспечением необходимой безопасности этих ресурсов; известных большому числу пользователей.

Расширение сферы влияния электронного бизнеса положительно влияет на развитие методов и средств управления доступом, что, в свою очередь, позитивно сказывается на развитии электронного бизнеса. В процессе современного развития инфраструктуры управления доступом можно выделить три фазы [7].

Первую фазу развития можно охарактеризовать как *обычный доступ к информации*, когда организации раскрывают для себя выгоды использования Интернета как рентабельного механизма для обмена информацией с клиентурой — т. е. сотрудниками, клиентами и партнерами. Сети интранет и экстранет разворачиваются как каналы для передачи конфиденциальной и персонифицированной информации.

Вторая фаза развития — это *расширенный корпоративный доступ*, когда организации доводят внутренние бизнес-процессы до Сети, предоставляя возможность таким пользователям, как сотрудники, клиенты и партнеры, участвовать в бизнес-процессах путем самообслуживания.

Третью фазу развития можно назвать *совместной коммерцией*, в которой компании распространяют свои внутренние бизнес-процессы че-

рез многие организации и сервис-провайдеров. Между организациями распространяются частный контент, являющийся собственностью конкретной организации, и транзакции, что требует обеспечения высокого уровня безопасности.

12.1.1. Методы управления удаленным доступом

В распределенной корпоративной сети обычно применяются два метода управления удаленным доступом:

- управление сетевым доступом;
- управление веб-доступом.

Каждый из этих методов является комплементарным по отношению к другому.

Управление сетевым доступом регулирует доступ к ресурсам внутренней сети организации. Управление веб-доступом регулирует доступ к веб-серверам и их содержимому.

Все запросы на доступ к ресурсам проходят через один или более списков контроля доступа ACL (Access Control List). Список контроля доступа ACL является набором правил доступа, которые задают для набора защищаемых ресурсов. Ресурсы с низким риском будут иметь менее строгие правила доступа, в то время как высококритичные ресурсы должны иметь более строгие правила доступа. Списки контроля доступа ACL, по существу, определяют политику безопасности.

Доступ к сетевым ресурсам организации можно регулировать путем создания списков контроля доступа Login ACL, которые позволяют точно определить конкретные разрешения и условия для получения доступа к ресурсам внутренней сети.

Средства контроля и управления веб-доступом позволяют создавать и исполнять политику веб-доступа. Создавая конкретные списки контроля веб-доступа Web ACL, администраторы безопасности определяют, какие пользователи могут получить доступ к веб-серверам организации и их содержимому и при каких заранее установленных условиях.

По определению, электронный бизнес предоставляет данные о бизнес-процессе своей организации через Сеть как своим сотрудникам, так и внешней клиентуре. Поэтому для организации очень важно сформировать доверие каждого пользователя к оперативному и обоснованному предоставлению веб-доступа к критически важным ресурсам и данным. При отсутствии всестороннего решения задачи управления веб-доступом эта проблема может быстро превратиться в административную катастрофу и разрушить электронный бизнес организации.

Управление доступом устанавливает и проводит в жизнь политики, которые контролируют права пользователя. Управление веб-доступом основывается на бизнес-правилах, которые определяют, какие пользователи могут получить доступ и к каким веб-ресурсам. Когда пользова-

тели пытаются получить доступ к конкретному приложению или некоторой области веб-сайта, доступ будет предоставлен или пользователю будет отказано в зависимости от того, удовлетворяет ли профиль полномочий данного пользователя определенным критериям. Эти критерии могут быть либо статическими — служебные обязанности или подразделение пользователя, — либо динамическими — состояние учетной записи (Account Status) пользователя.

В зависимости от разрешающей способности управления различают три уровня управления веб-доступом:

- низкая разрешающая способность (Coarse-grained);
- средняя разрешающая способность (Medium-grained);
- высокая разрешающая способность (Fine-grained).

Авторизация *с низкой разрешающей способностью* ограничивает доступ на уровне унифицированного указателя информационного ресурса URL (Uniform Resource Locator) с целью защиты машины и ее содержимого. Для блокирования хакеров или конкурентов можно контролировать доступ, основываясь на доменном имени пользователя в Интернете или на IP-адресе.

Авторизация *со средней разрешающей способностью* обеспечивает доступ к каталогам и файлам, основанный на списках контроля доступа. Этот уровень авторизации может быть осуществлен либо на базе индивидуальных и групповых списков контроля доступа, имеющихся на веб-сервере, либо на базе полномочий пользователя и групп, хранящихся в операционной системе. Обычно законный пользователь должен принадлежать к определенной группе для того, чтобы получить доступ к конкретному ресурсу и, в частности, к конкретной зоне сайта.

Авторизация *с высокой разрешающей способностью* обеспечивает детально проработанный контроль доступа, основанный на правилах. Такой контроль доступа требует использования интеллектуального централизованного управления (Policy Management) серверами, основанного на политиках компании. Такие серверы обладают способностью идентифицировать роль пользователя и применять сложные импликативные (if-then) правила бизнеса. Продукты для авторизации с высокой разрешающей способностью могут обеспечивать управление с высоким уровнем разрешения. Администраторы могут предоставлять доступ или отказывать в нем конкретным транзакциям, ограничивая не только ресурсы, доступные пользователям, но также и функции, которые они могли бы выполнить в данном приложении [7].

Управление доступом в гетерогенной среде требует от администраторов безопасности управления большим числом регистрационных записей пользователей и связанных с ними полномочий, идентификации каждого пользователя и затем разрешения доступа к ресурсам на основе проверки полномочий пользователя. Некоторые операционные системы, веб-серверы и приложения предоставляют ограниченные сервисы управления доступом. Однако для крупномасштабного применения с авторизацией с высокой разрешающей способностью такие фрагментарные решения нецелесообразны.

Управление доступом упрощается при применении единой централизованной инфраструктуры контроля и управления доступом. Такие централизованные инфраструктуры управления доступом могут разрешить пользователям самообслуживание, поручая им такие задачи управления, как регистрация, редактирование профиля, восстановление пароля и управление подпиской. Они могут также обеспечить делегирование администрирования, передачу функций управления пользователями людям, наиболее осведомленным о конкретной группе пользователей — как внутри, в бизнес-подразделениях организации, так и вне — у клиентов и в подразделениях бизнес-партнеров. Чтобы облегчить поддержку системы безопасности масштаба предприятия, средства управления доступом могут получать данные пользователей и политик, уже хранимые в таких хранилищах данных, как каталоги LDAP и реляционные базы данных.

12.1.2. Функционирование системы управления доступом

Централизованные системы управления доступом выпускаются рядом компаний, в частности Secure Computing, RSA Security Inc., Baltimore и др.

Рассмотрим функционирование системы управления доступом на примере системы PremierAccess компании Secure Computing. Программная система управления доступом PremierAccess осуществляет управление веб- и сетевым доступом всех пользователей, включая внутренних пользователей, удаленных сотрудников, клиентов, поставщиков и бизнес-партнеров. Данная система базируется на политике безопасности, которая позволяет персонализировать права доступа пользователей. Пользователи получают доступ только к тем ресурсам, на которые было дано разрешение в соответствии с их правами доступа, через веб-, VPN- или удаленный доступ с использованием серверов RADIUS. Система использует мультисерверную архитектуру и технологии, основанные на стандартах, чтобы обеспечить надежный контроль серверов и их содержимого.

Для того чтобы объективно идентифицировать пользователей, прежде чем им будет разрешен доступ к защищаемым ресурсам организации, в системе реализованы основанные на применении каталогов процессы аутентификации, авторизации и администрирования действий пользователей. Система поддерживает различные типы аутентификаторов — от многоразовых паролей до биометрических средств аутентификации. Предпочтение отдается методам и средствам строгой аутентификации.

Средства управления пользователями позволяют управлять большим числом пользователей. Сервер регистрации дает возможность самим пользователям регистрироваться в сети, используя стандартные веб-браузеры.

В процессе регистрации пользователям назначаются роли. Роли являются ярлыками, идентифицирующими группы пользователей, которые разделяют одинаковые права доступа. Иначе говоря, роли определяют наборы правил доступа, применяемых к конкретным группам пользователей. Категорирование пользователей по ролям можно выполнить на основе их функциональных обязанностей. Например, можно установить роли для сотрудников административного аппарата, отдела маркетинга, бухгалтерии и т. д. Для создания ролей можно применять и другие признаки категорирования. Все роли должны быть связаны с поддерживающим списком контроля доступа ACL, чтобы каждое значение нашло отражение в политике безопасности.

Переход от обычного пользовательского к ролевому управлению с предварительно установленными ограничениями дает возможность справиться с требованиями доступа всех пользователей. Универсальный веб-агент регулирует доступ к любому веб-серверу на базе ОС Solaris или Windows. Компонент PKI поддерживает промышленный стандарт сертификатов X.509, веб-регистрацию пользователей, многоразовые пароли, аутентификацию, основанную на аппаратных и программных аутентификаторах.

Рассмотрим работу средств управления сетевым доступом и веб-доступом.

Средства управления сетевым доступом

В системе управления доступом используются так называемые агенты. Агент системы — это программный модуль, установленный на соответствующий сервер в рамках корпоративной сети (рис. 12.2).

В качестве таких агентов выступают агенты удаленного доступа, VPN-доступа, серверов Radius, Novel, RAS, Citrix и др. При попытке пользователя подключиться к внутренней сети агенты системы перехватывают запрос пользователя на вход в сеть.

Агенты действуют как точки аутентификации пользователей UAP (User Authentication Point) на линиях коммуникации с сервером PremierAccess. В ответ на запрос пользователя агент запрашивает у пользователя его верительные данные — идентификатор пользователя и аутентификатор. Отвечая на запрос агента, пользователь вводит свои данные. Эти верительные данные передаются AAA-серверу (AAA — Authentication, Authorization, Accounting).

AAA-сервер сравнивает идентификатор ID пользователя или сертификат с данными, хранимыми в каталоге LDAP, с целью проверки их тождественности. Если идентификатор ID пользователя совпадает с хранимым, запись пользователя в базе данных проверяется по роли (или ролям) и ресурсам, к которым они авторизуются. Для аутентификации могут применяться фиксированный пароль, аппаратный или программный аутентификаторы. Если пользователь успешно проходит

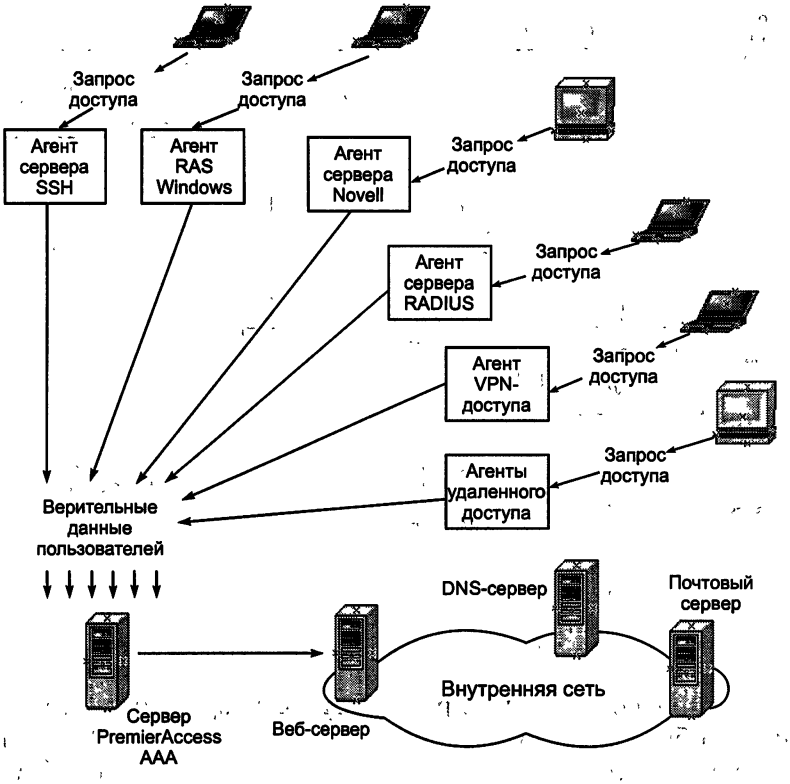


Рис. 12.2. Схема управления доступом к сети

все шаги подтверждения своей подлинности, он получает доступ к ресурсу сети.

Средства управления веб-доступом

Система PremierAccess использует универсальный веб-агент UWA (Universal Web Agent), который устанавливается на хост-машине каждого защищаемого веб-сервера. В рассматриваемом примере в качестве пользователя выступает бизнес-партнер, который запрашивает доступ к защищаемому веб-ресурсу компании (рис. 12.3).

Управление веб-доступом реализуется в виде процесса, состоящего из двух этапов.

На первом этапе пользователь пытается войти в систему, используя сервер WLS (Web Login Server). Запрос пользователя на доступ к защищенному веб-ресурсу компании перехватывается агентом UWA, который для обработки этого запроса обращается к серверу WLS. Сервер WLS запрашивает результат аутентификации у сервера AAA. В случае успешной аутентификации сервер WLS генерирует сеансовый cookie, который содержит сеансовый идентификатор пользователя.

Второй этап этого процесса начинается, когда пользователь пытается получить доступ к веб-ресурсу. Сервер WLS использует сеансовый

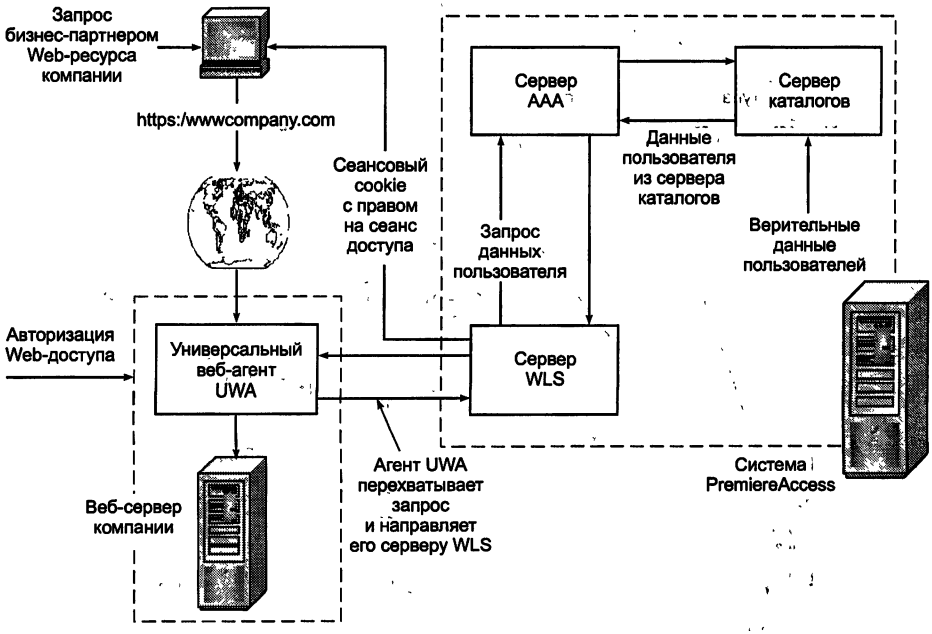


Рис. 12.3. Схема управления веб-доступом

идентификатор в cookie для запроса у AAA-сервера данных сеанса пользователя. Чтобы выполнить запрос на доступ, сервер WLS передает пользователю сеансовый cookie с правами на сеанс. Агент UWA получает сеансовый ID, а затем получает от AAA-сервера данные сеанса. Основываясь на ролях пользователя и политике доступа, он принимает решение, дать или запретить данному пользователю доступ к веб-ресурсу.

При построении систем управления удаленным доступом важное значение имеют следующие средства и системы:

- средства и протоколы аутентификации удаленных пользователей;
- инфраструктуры управления открытыми ключами PKI.

Инфраструктура управления открытыми ключами PKI была рассмотрена в главе 4.

Средства и протоколы аутентификации удаленных пользователей рассматриваются в последующих разделах данной главы.

12.2. Организация защищенного удаленного доступа

Удаленный доступ к компьютерным ресурсам стал в настоящее время таким же актуальным и значимым, как и доступ в режиме непосредственного подключения. Удаленный доступ к корпоративной сети осуществляется из незащищенного внешнего окружения через открытые сети. Поэтому средства построения защищенной корпоративной сети должны обеспечить безопасность сетевого взаимодействия при подключении к сети удаленных компьютеров.

Удаленный доступ к корпоративной сети возможен через глобальную компьютерную сеть или через среду передачи информации, образованную цепочкой из локальной и глобальной компьютерных сетей. Доступ через глобальную сеть Интернет является достаточно эффективным способом удаленного доступа к корпоративной сети, причем для подключения удаленного пользователя к Интернету может использоваться, в частности, канал телефонной связи. Отметим основные достоинства удаленного доступа к корпоративной сети через Интернет:

- обеспечивается масштабируемая поддержка удаленного доступа, позволяющая мобильным пользователям связываться с интернет-провайдером и затем через Интернет входить в свою корпоративную сеть;
- сокращаются расходы на информационный обмен через открытую внешнюю среду, так как удаленные пользователи подключаются к Интернету и через эту глобальную сеть связываются с минимальными затратами с сетью своей организации;
- управление трафиком удаленного доступа осуществляется так же, как любым другим трафиком Интернета.

В корпоративной сети для взаимодействия с удаленными пользователями выделяется сервер удаленного доступа. Этот сервер служит для выполнения следующих функций:

- установки соединения с удаленным компьютером;
- аутентификации удаленного пользователя;
- управления удаленным соединением;
- посредничества при обмене данными между удаленным компьютером и корпоративной сетью.

Среди протоколов удаленного доступа к локальной сети наибольшее распространение получил протокол точка—точка PPP (Point-to-Point Protocol), который является открытым стандартом Интернета. Протокол PPP предназначен для установления удаленного соединения и обмена информацией по установленному каналу пакетами сетевого уровня, инкапсулированными в PPP-кадры. Используемый в протоколе PPP метод формирования кадров обеспечивает одновременную работу через канал удаленной связи нескольких протоколов сетевого уровня.

Протокол PPP поддерживает следующие важные функции:

- аутентификацию удаленного пользователя и сервера удаленного доступа;
- компрессию и шифрование передаваемых данных;
- обнаружение и коррекцию ошибок;
- конфигурирование и проверку качества канала связи;
- динамическое присвоение адресов IP и управление этими адресами.

На основе протокола PPP построены часто используемые при удаленном доступе протоколы PPTP, L2F и L2TP. Эти протоколы позволяют создавать защищенные каналы для обмена данными между удаленными компьютерами и локальными сетями, функционирующими по различным протоколам сетевого уровня — IP, IPX или NetBEUI. Для передачи по телефонным каналам связи пакеты этих протоколов ин-

капсулируются в PPP-кадры. При необходимости передачи через Интернет защищенные PPP-кадры инкапсулируются в IP-пакеты сети Интернет. Криптозащита трафика возможна как в каналах Интернета, так и на протяжении всего пути между компьютером удаленного пользователя и сервером удаленного доступа локальной сети.

12.2.1. Средства и протоколы аутентификации удаленных пользователей

Контроль доступа пользователей к ресурсам корпоративной сети должен осуществляться в соответствии с политикой безопасности организации, которой принадлежит данная сеть. Эффективное разграничение доступа к сетевым ресурсам может быть обеспечено только при надежной аутентификации пользователей. Требования к надежности аутентификации удаленных пользователей должны быть особенно высокими. Это обусловлено тем, что при взаимодействии с физически удаленными пользователями значительно сложнее обеспечить доступ к сетевым ресурсам только для тех пользователей, которые имеют на это определенные полномочия. В отличие от локальных пользователей, удаленные пользователи не проходят процедуру физического контроля при допуске на территорию организации.

При удаленном взаимодействии важна аутентификация не только пользователей, но и оборудования, поскольку подмена пользователя или маршрутизатора приводит к одним и тем же последствиям — данные из корпоративной сети передаются не тем лицам, которым они предназначены.

Для обеспечения надежной аутентификации удаленных пользователей необходимо выполнение следующих требований:

- проведение аутентификации обеих взаимодействующих сторон — как удаленного пользователя, так и сервера удаленного доступа — для исключения маскировки злоумышленников;
- применение механизма одноразовых паролей для исключения перехвата и несанкционированного использования аутентифицирующей информации либо применение криптозащиты передаваемых секретных паролей;
- осуществление динамической аутентификации взаимодействующих сторон в процессе работы удаленного соединения;
- оперативное согласование используемых протоколов аутентификации.

Аутентификация на основе одноразовых паролей OTP

Технология аутентификации на основе одноразовых паролей OTP (One Time Password) обеспечивает возможность проверки подлинности удаленного пользователя, претендующего на получение доступа к защищаемым ресурсам системы.

Основным отличием данной технологии от аутентификации с использованием постоянных паролей заключается в том, что каждый раз пользователь должен вводить новое значение пароля.

Данная функциональная особенность обеспечивает защиту от возможного перехвата и повторного использования пароля нарушителем и позволяет применять ее в открытых сетях.

Примером алгоритма формирования одноразовых паролей является HOTP, разработанный Международной ассоциацией OATH (Open AuTHentication Group). Алгоритм использует в качестве входных значений секретный ключ K и текущее значение счетчика генераций N, который увеличивается при каждой новой генерации пароля.

Основной функциональный блок алгоритма HOTP вначале вычисляет значение согласно алгоритму HMAC-SHA-1, а затем выполняет операцию выделения (Truncate) из полученного 160-битного значения 6 цифр, являющихся одноразовым паролем:

$$\text{HOTP}(K, N) = \text{Truncate}(\text{HMAC-SHA-1}(K, N)),$$

где K — секретный ключ; N — счетчик генераций.

На рис. 12.4 показан пример генерации одноразовых паролей на стороне пользователя.

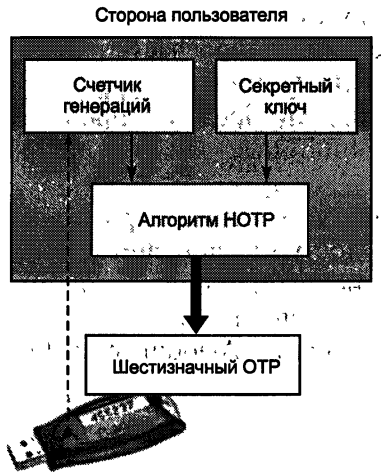


Рис. 12.4. Пример генерации одноразовых паролей на стороне пользователя

Генераторы одноразовых паролей можно реализовать двумя способами: программным и аппаратным. Первый из них, естественно, менее надежен. Дело в том, что клиентская утилита должна хранить в себе секретный ключ пользователя. Сделать это более или менее безопасно можно только с помощью шифрования самого ключа на основе персонального пароля. При этом необходимо учитывать, что клиентская утилита должна быть установлена на том устройстве (КПК, смартфоне и т. п.), с которого в данный момент выполняется сессия. Таким образом, получается, что аутентификация сотрудника зависит от одного па-

роля, при этом существует множество способов узнать или подобрать его. И это далеко не единственная уязвимость программного генератора одноразовых паролей. Существенно большей надежностью обладают аппаратные устройства для генерации одноразовых паролей OTP.

В основу технологии аутентификации на основе одноразовых паролей OTP заложены следующие компоненты:

- генератор одноразовых паролей, представляющий собой аппаратное устройство, предназначенное для формирования уникальных значений пароля по запросу пользователя;
- сервер доступа, обеспечивающий получение и первичную обработку одноразовых паролей, полученных от терминалов пользователей;
- сервер аутентификации RADIUS, обеспечивающий проверку прав доступа пользователей в соответствии с данными, полученными от сервера доступа.

Алгоритм практического использования технологии аутентификации на основе одноразовых паролей приведен ниже.

1. На первом этапе аутентификации пользователь генерирует одноразовый пароль при помощи аппаратного устройства и затем отправляет его по сети вместе со своим регистрационным именем серверу доступа.

2. Сервер доступа получает от пользователя регистрационное имя и значение пароля, после чего передает эти параметры по протоколу RADIUS серверу аутентификации.

3. Сервер аутентификации проводит проверку правильности предоставленных аутентификационных данных, результат которой отправляется серверу доступа.

4. На основе полученного ответа сервер доступа разрешает или запрещает пользователю доступ к запрашиваемому ресурсу.

Для реализации технологии аутентификации на основе одноразовых паролей в системе может использоваться система с генераторами паролей eToken NG-OTP компании Aladdin (рис. 12.5).

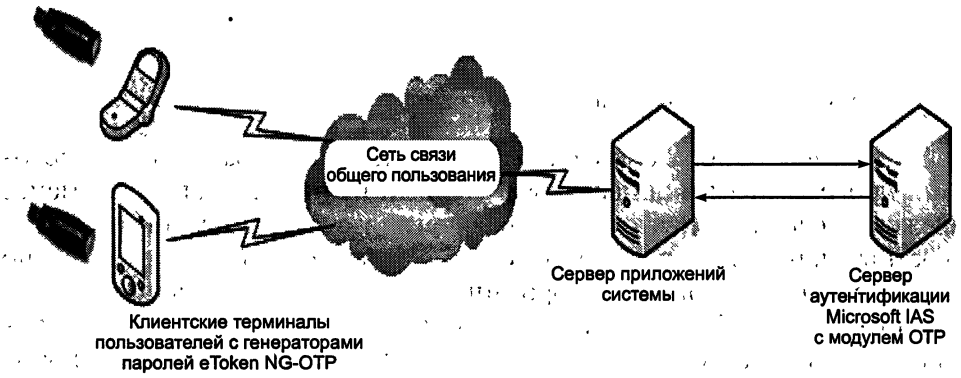


Рис. 12.5. Система аутентификации с генераторами паролей eToken NG-OTP компании Aladdin

Данная система включает в себя генераторы паролей eToken NG-OTP, реализующие алгоритм HOTP, а также сервер аутентификации Microsoft Internet Authentication Server (IAS) с установленным дополнительным модулем OTP.

В качестве сервера доступа в данном случае выступает сервер приложений, который обеспечивает взаимодействие с мобильными терминалами пользователей.

Достоинством данной системы является использование независимого, т. е. не требующего подключения к какому-либо устройству, клиентского средства на базе eToken. Это клиентское средство вырабатывает одноразовый пароль и высвечивает его на своем дисплее. Пользователю остается только ввести этот пароль с клавиатуры терминала.

Если же используется сервер RADIUS, отличный от Microsoft IAS, то в этом случае он может быть перенастроен в режим прокси, в котором он должен перенаправлять все поступающие к нему запросы на сервер Microsoft IAS с модулем OTP.

Основное назначение токенов заключается в мобильной аутентификации посредством одноразовых паролей. Самым большим их преимуществом по сравнению, например, с биометрическими методами распознавания является независимость от наличия специального аппаратного и программного обеспечения на терминале доступа — это обязательное требование со стороны мобильных пользователей, нуждающихся в безопасном доступе к корпоративным серверам из любой точки земного шара.

Концепция одноразовых паролей OTP в совокупности с современными криптографическими методами позволяет реализовать надежные системы удаленной аутентификации. Данная технология обладает рядом серьезных достоинств:

1. Надежность одноразовых паролей. Сегодня известно немного способов действительно сильной аутентификации пользователей при передаче информации по открытым каналам связи. Между тем такая задача встречается все чаще и чаще. Одноразовые пароли — одно из перспективных ее решений.

2. Использование стандартных криптографических алгоритмов. Это означает, что для реализации системы аутентификации с применением OTP подходят уже существующие разработки. Это наглядно доказывает ключ eToken NG-OTP, совместимый с отечественными криптоплагинами. Такие токены можно использовать в уже существующих системах корпоративной безопасности без их перестройки. В результате внедрение технологии одноразовых паролей можно провести с относительно небольшими затратами.

3. Защита слабо зависит от человеческого фактора. В аппаратных генераторах на базе USB-токенов используется полноценная двухфакторная аутентификация.

4. Удобство концепции OTP для пользователей. Получать доступ к необходимой информации с помощью одноразовых паролей ничуть не сложнее, чем применять для этой цели статичные ключевые слова. Не-

которые аппаратные реализации данной технологии можно использовать на любых устройствах, независимо от существующих на них портов и установленного ПО.

Протоколы аутентификации удаленных пользователей

Протокол PPP имеет встроенные средства, которые могут быть использованы для организации аутентификации при удаленном взаимодействии. Широко применяются следующие протоколы аутентификации:

- протокол доступа по паролю PAP;
- протокол аутентификации при рукопожатии CHAP;
- протокол расширенной аутентификации EAP.

В стандарте RFC 1334 определены протоколы PAP и CHAP. В стандарте RFC 3748 описан протокол EAP.

В процессе установления удаленного соединения каждая из взаимодействующих сторон может предложить применение одного из стандартных протоколов аутентификации — PAP, CHAP или EAP.

Следует отметить, что при использовании протокола PAP идентификаторы и пароли передаются по линии связи в незашифрованном открытом виде. При использовании протокола CHAP каждый пароль перед передачей по линии связи шифруется на основе случайного числа, полученного от сервера. Технология, применяемая в протоколе CHAP, обеспечивает также защиту от повторного использования злоумышленником перехваченных пакетов с зашифрованным паролем. Протокол EAP обладает наиболее широкими возможностями. Иногда компании создают собственные протоколы аутентификации удаленного доступа, работающие вместе с протоколом PPP. Эти фирменные протоколы обычно являются модификациями протоколов PAP, CHAP и EAP.

Протокол PAP

Суть работы протокола PAP (Password Access Protocol) довольно проста. В процессе аутентификации участвуют две стороны — проверяемая и проверяющая. Протокол PAP использует для аутентификации передачу проверяемой стороной идентификатора и пароля в виде открытого текста. Если проверяющая сторона обнаруживает совпадение идентификатора и пароля с записью, имеющейся у него в базе данных легальных пользователей, то процесс аутентификации считается успешно завершенным, после чего проверяемой стороне посылается соответствующее сообщение. В качестве стороны, чья подлинность проверяется, как правило, выступает удаленный пользователь, а в качестве проверяющей стороны — сервер удаленного доступа.

Для инициализации процесса аутентификации на базе протокола PAP сервер удаленного доступа после установления сеанса связи высы-

лает удаленному компьютеру пакет LCP (Link Control Protocol — протокол управления каналом), указывающий на необходимость применения протокола PAP. Далее осуществляется обмен пакетами PAP. Удаленный компьютер передает по каналу связи проверяющей стороне идентификатор и пароль, введенные удаленным пользователем. Сервер удаленного доступа по полученному идентификатору пользователя выбирает эталонный пароль из базы данных системы защиты и сравнивает его с полученным паролем. Если они совпадают, то аутентификация считается успешной, что сообщается удаленному пользователю. В целях безопасности на сервере чаще хранятся не пароли в открытом виде, а их хэш-значения.

Данная схема имеет существенный недостаток: любой злоумышленник, способный перехватывать сетевые пакеты, может получить пароль пользователя с помощью простейшего анализатора пакетов типа «сниффер». Получив этот пароль, злоумышленник легко пройдет аутентификацию под именем владельца пароля.

По сети в процессе аутентификации может передаваться не просто пароль, а результат его преобразования — скажем, тот же хэш пароля. К сожалению, это не устраняет описанный выше недостаток — злоумышленник с тем же успехом может перехватить хэш пароля и применять его впоследствии.

Следует особо отметить, что протокол аутентификации PAP, согласно которому идентификаторы и пароли передаются по линии связи в незашифрованном виде, целесообразно применять только совместно с протоколом, ориентированным на аутентификацию по одноразовым паролям, например S/Key.

Протокол CHAP

Протокол CHAP (Challenge-Handshake Authentication Protocol) относится к протоколам типа «запрос—ответ». В отличие от протокола PAP, в протоколе CHAP пароль каждого пользователя для передачи по линии связи шифруется на основе случайного числа, полученного от сервера. Такая технология обеспечивает не только защиту пароля от хищения, но и защиту от повторного использования злоумышленником перехваченных пакетов с зашифрованным паролем. Протокол CHAP применяется в современных сетях гораздо чаще, чем PAP, так как он использует передачу пароля по сети в защищенной форме и, следовательно, гораздо безопаснее [7].

Шифрование пароля в соответствии с протоколом CHAP выполняется с помощью криптографического алгоритма хэширования и поэтому является необратимым. В стандарте RFC 1334 для протокола CHAP в качестве хэш-функции определен алгоритм MD5, вырабатывающий из входной последовательности любой длины 16-байтное значение. Хотя минимальной длиной секрета является один байт, для повышения криптостойкости рекомендуется использовать секрет длиной не менее

16 байт. Спецификация CHAP не исключает возможность использования других алгоритмов вычисления хэш-функций.

Для инициализации процесса аутентификации по протоколу CHAP сервер удаленного доступа после установления сеанса связи должен выслать удаленному компьютеру пакет LCP, указывающий на необходимость применения протокола CHAP, а также требуемого алгоритма хэширования. Если удаленный компьютер поддерживает предложенный алгоритм хэширования, то он должен ответить пакетом LCP о согласии с предложенными параметрами. В противном случае выполняется обмен пакетами LCP для согласования алгоритма хэширования.

После этого начинается аутентификация на основе обмена пакетами протокола CHAP. Каждый пакет протокола CHAP включает четыре поля:

- поле «Код» (Code) указывает тип пакета;
- поле «Идентификатор» (Identifier) содержит уникальное число, которое позволяет определить, какому запросу соответствует полученный ответ;
- поле «Длина» (Length) указывает длину пакета в байтах;
- поле «Данные» (Data) — длина и формат этого поля определяются типом пакета CHAP.

В протоколе CHAP определены пакеты четырех типов:

- «Вызов» (Challenge);
- «Отклик» (Response);
- «Подтверждение» (Success);
- «Отказ» (Failure).

Протокол CHAP использует для аутентификации удаленного пользователя результат шифрования произвольного слова-вызова с помощью уникального секрета. Этот секрет имеется как у проверяющей, так и у проверяемой стороны. Процедура аутентификации начинается с отправки сервером удаленного доступа пакета «Вызов» (рис. 12.6). Поле данных в пакете «Вызов» содержит:

- произвольную числовую последовательность, которая должна быть уникальной для каждого посланного пакета «Вызов», а также длину этой последовательности в байтах;
- идентификатор проверяющей стороны.

Рис. 12.6. Шаги процесса аутентификации по протоколу CHAP

Удаленный компьютер, получив пакет «Вызов», зашифровывает его с помощью односторонней функции и известного ему секрета, получая в результате дайджест. Дайджест возвращается проверяющей стороне в виде пакета «Отклик».

Поле данных в этом пакете содержит следующие элементы:

- результат применения согласованного алгоритма хэширования над информационной структурой, состоящей из идентификатора проверяющей стороны и числовой последовательности из пакета «Вызов», а также секретного пароля удаленного пользователя;
- идентификатор проверяемой стороны, который может быть использован для того, чтобы проверяющая сторона могла отыскать в своей базе данных соответствующую пару идентификатор—секретный пароль.

Длина результата хэширования зависит от применяемой хэш-функции. Для алгоритма MD5 длина хэш-кода, а сответственно, и результата хэширования равна 128 бит. Так как используется односторонняя хэш-функция, то по перехваченным пакетам «Вызов» и «Отклик» вычислить пароль удаленного пользователя практически невозможно.

Получив пакет «Отклик», сервер удаленного доступа по идентификатору проверяемой стороны извлекает из базы данных системы защиты секретный эталонный пароль пользователя и выполняет согласованный алгоритм хэширования над информационной структурой, состоящей из его идентификатора и числовой последовательности, которые были посланы в пакете «Вызов», а также секретного эталонного пароля. Далее сервер сравнивает содержимое результата из полученного пакета «Отклик» с результатом, вычисленным самостоятельно. Если эти результаты совпадают, то аутентификация считается успешной и сервер высылает удаленному компьютеру пакет «Подтверждение».

В противном случае сервер удаленного доступа высылает пакет «Отказ» и разрывает сеанс связи. Поле данных в пакетах «Подтверждение» и «Отказ» включает соответствующее сообщение, содержание которого протоколом CHAP не устанавливается.

Пакет «Вызов» должен быть отправлен сервером повторно, если в ответ на него не был получен пакет «Отклик». Кроме того, пакет «Вызов» может отправляться периодически в течение сеанса удаленной связи для проведения динамической аутентификации, чтобы убедиться, что противоположная сторона не была подменена. Соответственно, пакет «Отклик» должен отправляться проверяемой стороной в ответ на каждый принятый пакет «Вызов».

Для защиты от перехвата ответа сервер удаленного доступа должен использовать различные значения слова-вызова при каждой следующей аутентификации. Из схемы аутентификации по протоколу CHAP становится понятно, что числовая последовательность в пакете «Вызов» должна быть уникальной и непредсказуемой. Если данная последовательность не будет уникальной, то злоумышленник сможет повторно

использовать перехваченный ранее пакет «Отклик», маскируясь под санкционированного удаленного пользователя.

Для того чтобы числовая последовательность в пакете «Вызов» была уникальной и непредсказуемой, в большинстве реализаций протокола CHAP она формируется как конкатенация двух элементов — текущего времени, включая время в секундах, дату и год, а также сгенерированного случайного числа.

Следует отметить, что протоколы типа «запрос—ответ» легко расширяются до схемы взаимной аутентификации.

При аутентификации по протоколу CHAP иногда возникают проблемы несовместимости узлов сети, которые порождаются использованием нестандартных функций вычисления дайджеста. Например, компания «Майкрософт» реализовала собственный вариант протокола, названный ею MS-CHAP, в котором используется дайджест-функция, отличная от MD5. И если сервер удаленного доступа Microsoft RAS сконфигурирован на собственный зашифрованный вариант аутентификации при удаленном доступе (выбрана опция **Microsoft encrypted authentication**), то удаленные пользователи, работающие со стандартным клиентским программным обеспечением PPP, не смогут пройти аутентификацию на этом сервере.

Протокол EAP

Протокол EAP (Extensible Authentication Protocol) предназначен для обеспечения расширенной аутентификации. Протокол EAP позволяет проверять подлинность при подключениях удаленного доступа с помощью различных механизмов проверки подлинности. Точная схема проверки подлинности согласовывается клиентом удаленного доступа и сервером, выполняющим проверку подлинности. Им может быть сервер удаленного доступа или сервер RADIUS.

Особенностью данного протокола является то, что механизм аутентификации определяется на более поздней фазе, уже после установления непосредственного соединения. Это позволяет проверяющему серверу получить некую дополнительную информацию о клиенте, который хочет быть авторизован.

Протокол EAP позволяет осуществлять процесс аутентификации в виде диалога между клиентом удаленного доступа и системой проверки подлинности. Такой диалог состоит из запросов системы проверки подлинности на необходимую ей информацию и ответов клиента удаленного доступа.

Определим основные термины, которые будут использованы при описании процесса аутентификации по протоколу EAP:

- *аутентификатор (Authenticator)* — один из концов соединения, требующий аутентификации;
- *клиент (Peer)* — другой конец соединения, который будет проходить процесс аутентификации на аутентификаторе.

Рассмотрим процесс аутентификации в соответствии с протоколом EAP.

1. После процедуры установления соединения аутентификатор посылает запрос клиенту, в котором содержится поле «Тип», — оно показывает, что именно запрашивает аутентификатор. Запрос может посылаться несколько раз.

2. Затем клиент посылает пакет с ответом аутентификатору, причем на каждый из запросов. В ответе также содержится поле «Тип», указывающее, на какой именно запрос дается ответ.

3. Аутентификатор заканчивает процедуру аутентификации, посылая клиенту пакет, сигнализирующий об успешной (Success Packet) или о неудавшейся аутентификации (Failure Packet).

Последовательность пунктов 1—2 может повторяться необходимое число раз, определяемое реализацией. При этом протокол EAP является пошаговым (Lock-step), т. е. каждый последующий пакет с запросом посылается только после получения ответа на предыдущий запрос.

Например, сервер, выполняющий проверку подлинности, может запрашивать у клиента удаленного доступа имя пользователя, идентификатор и код доступа. После ответа на каждый такой запрос клиент удаленного доступа проходит определенный уровень проверки подлинности. Когда на все запросы будут получены удовлетворительные ответы, проверка подлинности клиента удаленного доступа успешно завершается.

Схемы проверки подлинности, использующие протокол EAP, называются *типами EAP*. По умолчанию поддерживается два типа EAP (MD5-задача и EAP-TLS). Для успешной проверки подлинности клиент удаленного доступа и сервер, выполняющий проверку подлинности, должны поддерживать один и тот же тип EAP. Подключение других модулей EAP к серверу, использующему маршрутизацию и удаленный доступ, обеспечивает поддержку других методов EAP.

Инфраструктура EAP для Microsoft Windows

EAP является набором встроенных компонентов, реализующих архитектурную поддержку любых типов EAP, выполненных в виде подключаемых модулей. EAP обеспечивает согласованность обработки всех элементов процесса аутентификации — от паролей до аутентификационных процедур типа «запрос—ответ» и сертификатов инфраструктуры открытого ключа.

Семейство Windows Server 2003 поддерживает два типа EAP (MD5-задача и EAP-TLS) и возможность передачи сообщений EAP серверу RADIUS (EAP-RADIUS). Можно также установить дополнительные типы EAP.

MD5-задача. MD5-задача (Message Digest 5 Challenge, MD5-Challenge) является обязательным типом EAP, который использует тот же протокол обмена запросами, что и основанный на PPP протокол

CHAP, но запросы и ответы отправляются в виде сообщений EAP. Обычно MD5-задача применяется для проверки учетных данных клиентов удаленного доступа системами, использующими имя пользователя и пароль. Кроме того, с помощью MD5-задачи можно проверять работу EAP.

EAP-TLS. Протокол EAP-TLS (EAP-Transport Level Security) — это тип EAP, применяемый в системах безопасности, использующих сертификаты. Если проверка подлинности при удаленном доступе осуществляется с помощью смарт-карт, необходимо использовать метод проверки подлинности EAP-TLS. Обмен сообщениями EAP-TLS позволяет выполнять взаимную проверку подлинности, согласование метода шифрования и определение зашифрованного ключа между клиентом удаленного доступа и сервером, выполняющим проверку подлинности.

Протокол EAP-TLS обеспечивает самый надежный способ проверки подлинности и определения ключа.

Протокол EAP-TLS поддерживается только на серверах, на которых выполняется служба маршрутизации и удаленного доступа, использующих проверку подлинности Windows или RADIUS.

EAP-RADIUS. EAP-RADIUS — это не тип EAP, а способ передачи системой проверки подлинности серверу RADIUS сообщений EAP любого типа EAP. Например, для сервера удаленного доступа, настроенного на проверку подлинности RADIUS, сообщения EAP, пересылаемые между клиентом и сервером удаленного доступа, инкапсулируются и форматируются как сообщения RADIUS между сервером удаленного доступа и сервером RADIUS.

EAP-RADIUS применяется в системах, где используется служба проверки подлинности RADIUS. Преимущество EAP-RADIUS состоит в том, что типы EAP должны быть установлены только на сервере RADIUS, а не на каждом сервере удаленного доступа. В случае сервера IAS типы EAP требуется установить только на него.

Обычно при использовании EAP-RADIUS сервер, на котором выполняется маршрутизация и удаленный доступ, настроен на проверку подлинности с помощью протокола EAP и сервера IAS.

В процессе подключения клиент удаленного доступа согласовывает использование протокола EAP с сервером удаленного доступа. Когда клиент отправляет серверу удаленного доступа сообщение EAP, сервер удаленного доступа инкапсулирует сообщение EAP в виде сообщения RADIUS и отправляет его серверу IAS. Сервер IAS обрабатывает сообщение EAP и отправляет серверу удаленного доступа ответное сообщение EAP, инкапсулированное в виде сообщения RADIUS. Затем сервер удаленного доступа перенаправляет сообщение EAP клиенту удаленного доступа. В такой конфигурации сервер удаленного доступа является лишь посредником. Вся обработка сообщений EAP выполняется клиентом удаленного доступа и сервером IAS.

Будучи изначально предназначенным для использования вместе с PPP, протокол EAP нашел также широкое применение в беспроводных сетях (стандарт IEEE-802.1X).

Протокол S/Key

Одним из распространенных протоколов аутентификации на основе одноразовых паролей является стандартизованный в Интернете протокол S/Key (RFC 1760) [7]. Данный протокол реализован во многих системах, требующих проверки подлинности удаленных пользователей, в частности в системе TACACS+ компании Cisco.

Перехват одноразового пароля, передаваемого по сети в процессе аутентификации, не предоставляет злоумышленнику возможности повторно использовать этот пароль, так как при следующей проверке подлинности необходимо предъявлять уже другой пароль. Поэтому схема аутентификации на основе одноразовых паролей, в частности S/Key, позволяет передавать по сети одноразовый пароль в открытом виде и, таким образом, компенсирует основной недостаток протокола аутентификации PAP.

Однако следует отметить, что протокол S/Key не исключает необходимость задания секретного пароля для каждого пользователя. Этот секретный пароль используется только для генерации одноразовых паролей. Для того чтобы злоумышленник не смог по перехваченному одноразовому паролю вычислить секретный исходный пароль, генерация одноразовых паролей выполняется с помощью односторонней, т. е. необратимой, функции. В качестве такой односторонней функции в спецификации протокола S/Key определен алгоритм хэширования MD4 (Message Digest Algorithm 4). Некоторые реализации протокола S/Key в качестве односторонней функции используют алгоритм хэширования MD5 (Message Digest Algorithm 5).

Поясним основную идею протокола S/Key на следующем примере.

Пусть удаленному пользователю (проверяемой стороне) для регулярного прохождения аутентификации необходим набор из 100 одноразовых паролей.

Проверяемой стороне заранее назначается генерируемый случайный ключ K в качестве ее секретного постоянного пароля. Затем проверяющая сторона выполняет процедуру инициализации списка одноразовых $N = 100$ паролей. В ходе данной процедуры проверяющая сторона с помощью односторонней функции h вычисляет по ключу K проверочное значение w_{101} для первого одноразового пароля. Для вычисления значения w_{101} ключ K подставляют в качестве аргумента функции h и данная функция рекурсивно выполняется 101 раз:

$$w_1 = h(K),\ w_2 = h(h(K)),\ w_3 = h(h(h(K))),\ \ldots,$$

$$w_{101} = h(h(h(\ldots h(K)\ldots))) = h^{101}(K).$$

Идентификатор пользователя и соответствующий этому пользователю секретный ключ K, а также несекретные числа N и w_{101} сохраняются в базе данных проверяющей стороны. Число N является номером одноразового пароля для очередной аутентификации из списка одноразовых

паролей. Следует отметить, что после использования каждого такого одноразового пароля номер N уменьшается на единицу.

В процессе очередной аутентификации, проводимой после инициализации, проверяемая сторона предоставляет проверяющей стороне свой идентификатор, а та возвращает соответствующее этому идентификатору число N. В нашем примере $N = 100$. Затем проверяемая сторона вычисляет по своему секретному ключу K одноразовый пароль:

$$w'_{100} = h(h(h(...h(K))...))) = h^{100}(K)$$

и посылает его проверяющей стороне.

Получив значение w'_{100}, проверяющая сторона выполняет над ним один раз одностороннюю функцию $w'_{101} = h(w'_{100})$. Далее проверяющая сторона сравнивает полученное значение w'_{101} со значением w_{101} из базы данных. Если они совпадают, то это означает, что и $w'_{100} = w_{100}$ и, следовательно, аутентификация является успешной.

В случае успешной аутентификации проверяющая сторона заменяет в базе данных для проверяемой стороны число w_{101} на полученное от нее число w'_{100}, а число N на $N = N - 1$. С учетом того, что при успешной аутентификации номер одноразового пароля N для очередной аутентификации уменьшился на единицу, в базе данных проверяющей стороны совместно с идентификатором и секретным ключом K проверяемой стороны будут храниться числа $(N - 1)$ и w_{100}. Здесь под w_{100} понимается полученный от проверяемой стороны при успешной аутентификации последний одноразовый пароль. После использования очередного списка одноразовых паролей процедура инициализации должна выполняться снова.

Иногда желательно, чтобы пользователь имел возможность сам назначать секретный постоянный пароль. Для осуществления такой возможности спецификация S/Key предусматривает режим вычисления одноразовых паролей на основе не только секретного пароля, но и генерируемого проверяющей стороной случайного числа. Таким образом, в соответствии с протоколом S/Key за каждым пользователем закрепляется идентификатор и секретный постоянный пароль.

Перед тем как проходить аутентификацию, каждый пользователь должен сначала пройти процедуру инициализации очередного списка одноразовых паролей (иначе говоря, фазу парольной инициализации). Данная фаза выполняется по запросу пользователя на сервере удаленного доступа и состоит из следующих шагов:

1. У пользователя запрашивается его идентификатор.

2. Генерируется случайное несекретное число R, называемое кодом инициализации. Число R будет использоваться для вычисления одноразовых паролей пользователя до следующей парольной инициализации.

3. У пользователя запрашивается число одноразовых паролей (число N), как правило, из интервала $300 \le N \le 1000$, которое он предпола-

гает использовать до следующей парольной инициализации (данное число может также задаваться администратором заранее).

4. Из базы данных системы защиты по идентификатору пользователя извлекается его секретный пароль K.

5. Значения R и K используются как аргументы односторонней функции h, применяемой последовательно $N+1$ раз:

$$w_{N+1} = h(h(h(...(h(R, K))...))) = h^{N+1}(R, K).$$

6. Числа R, N и w_{N+1} сохраняются для пользователя в базе данных системы защиты вместе с его идентификатором и паролем. В отличие от пароля K, числа R, N и w_{N+1} не являются секретными.

Как уже отмечалось, число N является номером одноразового пароля для очередной аутентификации из списка возможных одноразовых паролей, причем этот номер N уменьшается на единицу после использования каждого такого пароля. Фаза парольной инициализации не требует передачи по сети секретного пароля и, соответственно, может быть активизирована пользователем как с компьютера локальной сети, так и с удаленной машины. После парольной инициализации пользователь может использовать N одноразовых паролей до следующей такой инициализации и, соответственно, устанавливать N сеансов удаленной связи с локальной сетью.

Процесс очередной аутентификации при удаленном доступе к локальной сети включает следующие шаги:

1. Удаленный пользователь сообщает серверу удаленного доступа свой идентификатор.

2. Из базы данных системы защиты по идентификатору пользователя сервер извлекает его секретный пароль K, а также числа R, N и w_{N+1}.

3. Сервер передает пользователю число R, которое для пользователя является постоянным до следующей инициализации, а также номер одноразового пароля N.

4. Пользователь на удаленном компьютере вводит секретный пароль K', и клиентское программное обеспечение вычисляет очередной одноразовый пароль:

$$w'_N = h(h(h(...(h(R, K'))...))) = h^N(R, K').$$

5. Вычисленный одноразовый пароль w'_N отправляется серверу удаленного доступа, который выполняет над ним один раз одностороннюю функцию h:

$$w'_{N+1} = h(w'_N).$$

6. Сервер сравнивает полученное значение w'_{N+1} со значением w_{N+1} из базы данных системы защиты. Если значения w'_{N+1} и w_{N+1} совпадают, то аутентификация считается успешной и удаленный пользователь допускается в локальную сеть; в противном случае посылается уведомление о неуспешной аутентификации и соединение разрывается.

7. В случае успешной аутентификации сервер заменяет в базе данных системы защиты для удаленного пользователя число w_{N+1} на полученный от него одноразовый пароль w'_N, а число N на $N = N - 1$; с учетом того, что номер одноразового пароля N для очередной аутентификации уменьшился на единицу, полученный от пользователя и занесенный в базу данных системы защиты одноразовый пароль будет теперь обозначаться как w_{N+1}.

Таким образом, при каждом новом запросе используется уникальный разовый пароль. При $N = 0$ параметры схемы генерируются заново [27, 73].

Основная цель злоумышленника заключается в раскрытии следующего одноразового пароля w_{i+1} по текущему w_i, т. е. сводится к вычислительно неразрешимой задаче обращения хэш-функции $w_{i+1} = h^{-1}(w_i)$. Для ускорения процедуры аутентификации определенное количество одноразовых паролей, например несколько десятков, может быть вычислено заранее и храниться на удаленном компьютере в зашифрованном виде.

Протокол аутентификации на основе одноразовых паролей S/Key применяют, в частности, для улучшения характеристик протоколов централизованного контроля доступа к сети удаленных пользователей TACACS+ и RADIUS.

12.2.2. Централизованный контроль удаленного доступа

Для управления удаленными соединениями небольшой локальной сети вполне достаточно одного сервера удаленного доступа. Однако если локальная сеть объединяет относительно большие сегменты и число удаленных пользователей существенно возрастает, то одного сервера удаленного доступа будет недостаточно.

При использовании в одной локальной сети нескольких серверов удаленного доступа требуется централизованный контроль доступа к компьютерным ресурсам.

Рассмотрим, как решается задача контроля доступа к сети удаленных пользователей в соответствии с обычной схемой, когда удаленные пользователи пытаются получить доступ к сетевым ресурсам, которые находятся под управлением нескольких разных операционных систем. Пользователь дозванивается до своего сервера удаленного доступа, и RAS выполняет для него процедуру аутентификации, например, по протоколу CHAP. Пользователь логически входит в сеть и обращается к нужному серверу, где снова проходит аутентификацию и авторизацию, в результате чего получает или не получает разрешение на выполнение запрошенной операции.

Нетрудно заметить, что такая схема неудобна пользователю, поскольку ему приходится несколько раз выполнять аутентификацию — при входе в сеть на сервере удаленного доступа, а потом еще всякий раз

при обращении к каждому ресурсному серверу сети. Пользователь вынужден запоминать несколько разных паролей. Кроме того, он должен знать порядок прохождения разных процедур аутентификации в различных операционных системах. Возникают также серьезные трудности с администрированием такой сети, администратор должен заводить учетную информацию о каждом пользователе на каждом сервере. Эти разрозненные базы данных трудно поддерживать в корректном состоянии. При увольнении сотрудника сложно исключить его из всех списков. Возникают проблемы при назначении паролей, существенно затрудняется аудит.

Отмеченные трудности и недостатки преодолеваются при установке в сети централизованной службы аутентификации и авторизации. Для централизованного контроля доступа выделяется отдельный сервер, называемый сервером аутентификации. Этот сервер служит для проверки подлинности удаленных пользователей, определения их полномочий, а также фиксации и накопления регистрационной информации, связанной с удаленным доступом. Надежность защиты повышается, если сервер удаленного доступа запрашивает необходимую для аутентификации информацию непосредственно у сервера, на котором хранится общая база данных системы защиты компьютерной сети.

Однако в большинстве случаев серверы удаленного доступа нуждаются в посреднике для взаимодействия с центральной базой данных системы защиты, например со службой каталогов. Это обусловлено тем, что стандартами удаленной аутентификации, поддерживаемыми серверами удаленного доступа, являются протоколы CHAP и PAP, которые не подходят без дополнений для аутентификации с использованием NDS (Novell Directory Services) или доменной службы Windows NT. Для проверки ответа на вызов сервера, поступившего от проходящего аутентификацию пользователя, реализация протокола CHAP применяет незашифрованную копию пароля в простой текстовой форме. При аутентификации на основе протокола PAP пароль также используется в открытом виде.

Большинство сетевых операционных систем и служб каталогов сохраняют эталонные пароли пользователей с использованием одностороннего хэширования, что не позволяет серверам удаленного доступа, стандартно реализующим протоколы PAP и CHAP, извлечь открытый эталонный пароль для проверки ответа.

Роль посредника во взаимодействии между серверами удаленного доступа и центральной базой данных системы защиты может быть возложена на сервер аутентификации. Централизованный контроль удаленного доступа к компьютерным ресурсам с помощью сервера аутентификации выполняется на основе специализированных протоколов. Данные протоколы позволяют объединять используемые серверы удаленного доступа и сервер аутентификации в одну подсистему, выполняющую все функции контроля удаленных соединений на основе взаимодействия с центральной базой данных системы защиты. Сервер аутентификации создает единую точку наблюдения и проверки всех удаленных пользова-

телей и контролирует доступ к компьютерным ресурсам в соответствии с установленными правилами.

К наиболее популярным протоколам централизованного контроля доступа к сети удаленных пользователей относятся протоколы TACACS (Terminal Access Controller Access Control System) и RADIUS (Remote Authentication Dial-In User Service). Системы TACACS и RADIUS предназначены в первую очередь для организаций, в центральной сети которых используется несколько серверов удаленного доступа. В этих системах администратор может управлять базой данных идентификаторов и паролей пользователей, предоставлять им привилегии доступа и вести учет обращений к системным ресурсам [7].

Протоколы TACACS и RADIUS требуют применения отдельного сервера аутентификации, который для проверки подлинности пользователей и определения их полномочий может не только использовать собственную базу данных, но и взаимодействовать с современными службами каталогов, например с NDS и Microsoft Windows NT Directory Service. Серверы TACACS и RADIUS выступают в качестве посредников между серверами удаленного доступа, принимающими звонки от пользователей, с одной стороны, и сетевыми ресурсными серверами — с другой. Реализации TACACS и RADIUS могут также служить посредниками для внешних систем аутентификации.

Рассмотрим особенности централизованного контроля удаленного доступа на примере протокола TACACS (рис. 12.7).

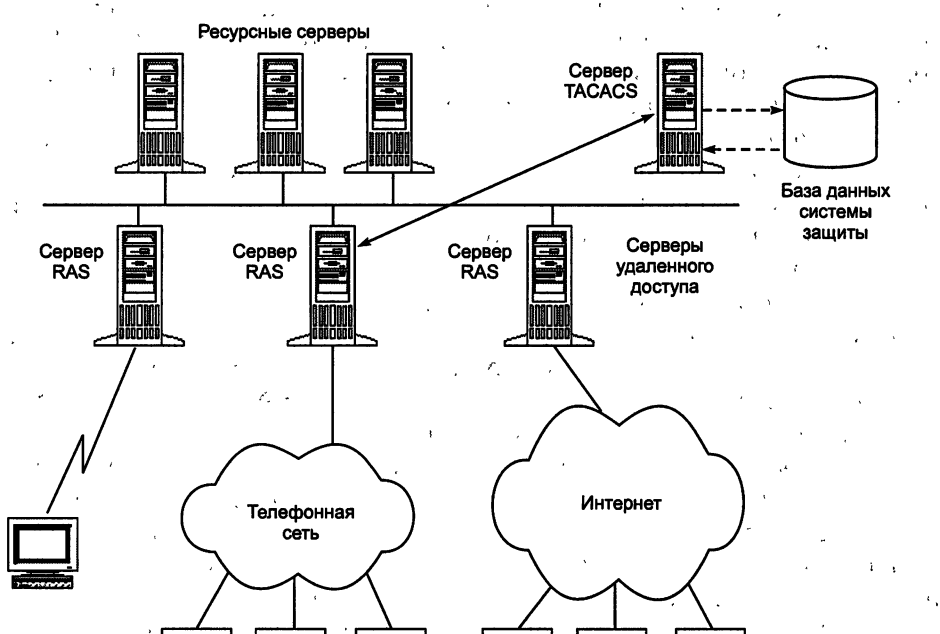


Рис. 12.7. Схема централизованного контроля удаленного доступа

Система TACACS выполнена в архитектуре клиент/сервер [27, 41]. В компьютерной сети, включающей несколько серверов удаленного доступа, устанавливается один сервер аутентификации, который называют сервером TACACS (обычно это программа, работающая в среде универсальной ОС, чаще всего UNIX).

На сервере TACACS формируется центральная база учетной информации об удаленных пользователях, включающая их имена, пароли и полномочия. В полномочиях каждого пользователя задаются подсети, компьютеры и сервисы, с которыми он может работать, а также различные виды ограничений, например временные ограничения. На этом сервере ведется база данных аудита, в которой накапливается регистрационная информация о каждом логическом входе, продолжительности сессии, а также времени использования ресурсов сети.

Клиентами сервера TACACS являются серверы удаленного доступа, принимающие запросы на доступ к ресурсам сети от удаленных пользователей. На каждый такой сервер установлено программное обеспечение, реализующее стандартный протокол, по которому они взаимодействуют с сервером TACACS. Этот протокол также называется TACACS.

Протокол TACACS стандартизует схему взаимодействия серверов удаленного доступа с сервером TACACS на основе задания возможных типов запросов, ответов и соединений. Определены запросы, с которыми клиенты могут обращаться к серверу TACACS. Сервер на каждый запрос должен ответить соответствующим сообщением. Протокол задает несколько типов соединений, каждое из которых определяется как последовательность пар запрос—ответ, ориентированная на решение отдельной задачи.

Определено три типа соединений:

- AUTH — выполняется только аутентификация;
- LOGIN — выполняется аутентификация и фиксируется логическое соединение с пользователем;
- SLIP — выполняется аутентификация, фиксируется логическое соединение, подтверждается IP-адрес клиента.

С помощью соединения AUTH серверы удаленного доступа перенаправляют серверу TACACS поток запросов на логическое подключение пользователей к сети в целом. Соединение LOGIN служит для перенаправления запросов серверу TACACS на логическое подключение пользователей к отдельным компьютерам локальной сети.

При соединении AUTH сервер удаленного доступа посылает на сервер TACACS только одно сообщение — пакет AUTH, на который сервер TACACS отвечает сообщением REPLY. Пакет AUTH имеет формат

(*username*, *password*, *line*, *style*),

где *username* — имя пользователя;

password — пароль пользователя (открытый текст);

line — номер порта сервера удаленного доступа, по которому пользователь установил соединение;

style — способ аутентификации.

Сервер TACACS на основании имеющихся у него данных проверяет пароль и возвращает ответ в виде пакета REPLY, где сообщает об успехе или неуспехе аутентификации. Сервер TACACS может выполнять аутентификацию самостоятельно или обращаться к другим системам аутентификации, например к системам аутентификации ОС UNIX, системе NDS ОС NetWare, системе Directory Services ОС Windows NT и т. п. В соответствии с протоколом TACACS пароль передается между сервером удаленного доступа и сервером аутентификации в открытом виде. Поэтому протокол TACACS необходимо применять совместно с протоколом аутентификации по одноразовым паролям, например S/Key.

Соединение LOGIN состоит в следующем обмене пакетов:

- при установлении логического соединения:
  - клиент отправляет пакет LOGIN;
  - сервер отвечает пакетом REPLY;
- при подключении к конкретному компьютеру (0 или более раз):
  - клиент отправляет пакет CONNECT;
  - сервер отвечает пакетом REPLY;
- для завершения сессии:
  - клиент отправляет пакет LOGOUT;
  - сервер отвечает пакетом REPLY.

Запрос LOGIN имеет следующий формат: (*username*, *password*, *line*). Значения полей те же, что и в запросе AUTH. Ответ сервера всегда имеет вид (*result1*, *result2*, *result3*), где все три поля — это целые числа, значение которых в протоколе не оговаривается. Эти числа могут интерпретироваться в соответствии с соглашением, принятым конкретным типом сервера удаленного доступа и сервером TACACS. Например, в серверах удаленного доступа Cisco поле *result3* интерпретируется как номер списка прав доступа, который нужно применить к данному пользователю. На основании полученных от сервера TACACS указаний сервер удаленного доступа выполняет процедуру аутентификации и разрешает или не разрешает удаленному пользователю логически войти в сеть.

При работе в сети пользователь может захотеть подключиться к разным компьютерам и приложениям. Каждый раз при этом сервер удаленного доступа обращается с запросом CONNECT к серверу TACACS. Запрос CONNECT имеет вид (*username*, *password*, *line*, *destination IP*, *destination Port*), где назначение первых трех полей — то же, что и в предыдущих запросах. Два последних поля идентифицируют IP-адрес компьютера назначения и TCP-порт, приложения, с которым устанавливается связь. Запрос CONNECT передается при уже установленном соединении с пользователем, и поэтому пароль в нем обычно не указывается. Запрос нужен для получения разрешения пользователю подключиться к указанному компьютеру по указанному IP-адресу. Ответ сервера имеет тот же вид, что и для запроса LOGIN.

Запрос LOGOUT передается для уведомления сервера TACACS о завершении сессии пользователя. Сервер ответом подтверждает прием уведомления.

С помощью приведенных сообщений серверы удаленного доступа перенаправляют поток запросов серверу TACACS на логическое подключение пользователей к сети в целом или к отдельным ее ресурсам.

Сервер TACACS может выполнять аутентификацию и авторизацию удаленных пользователей различными способами:

- с помощью встроенного механизма аутентификации той ОС, под управлением которой работает сервер;
- с помощью централизованных справочных систем ОС: NIS или NIS+ для ОС UNIX, NDS ОС NetWare, Directory Services ОС Windows NT и др.;
- с помощью систем аутентификации, основанных на одноразовых паролях (например, SecurID);
- путем передачи запросов другим системам аутентификации, например системе Kerberos.

Следует отметить, что недостатки протокола TACACS, связанные с открытой передачей пароля по сети, устранены компанией Cisco в версии, названной TACACS+.

В соответствии с протоколом TACACS+ пароль для передачи по сети шифруется с помощью алгоритма MD5. TACACS+ предусматривает раздельное хранение баз данных аутентификационной, авторизационной и учетной информации, в том числе и на разных серверах. Улучшено взаимодействие с системой Kerberos. Компания Cisco поддерживает в настоящее время в своих маршрутизаторах и серверах удаленного доступа усовершенствованную версию протокола TACACS+ [7].

Другой распространенной системой централизованной аутентификации при удаленном доступе является система RADIUS. По своим возможностям протоколы TACACS и RADIUS практически эквивалентны и являются открытыми стандартами, однако протокол RADIUS более популярен среди производителей систем централизованного контроля удаленного доступа. Это связано с тем, что основанное на нем серверное программное обеспечение распространяется бесплатно. Кроме того, протокол RADIUS менее сложен в реализации. В частности, для взаимодействия между сервером удаленного доступа и сервером аутентификации в протоколе TACACS используется протокол TCP, а в протоколе RADIUS — более простой, хотя и менее надежный протокол UDP.

12.3. Протокол Kerberos

Протокол Kerberos используется в системах клиент/сервер для аутентификации и обмена ключевой информацией, предназначенной для установления защищенного канала связи между абонентами, работающими как в локальной сети, так и в глобальных. Данный протокол

встроен в качестве основного протокола аутентификации в Microsoft Windows 2000 и в UNIX BSD.

Kerberos обеспечивает аутентификацию в открытых сетях, т. е. при работе Kerberos подразумевается, что злоумышленники могут производить следующие действия:

- выдавать себя за одну из легитимных сторон сетевого соединения;
- иметь физический доступ к одному из участвующих в соединении компьютеров;
- перехватывать любые пакеты, модифицировать их и/или передавать повторно.

Соответственно, обеспечение безопасности в Kerberos построено таким образом, чтобы нейтрализовать любые потенциальные проблемы, которые могут возникнуть из-за указанных действий злоумышленников.

Создание Kerberos велось в рамках проекта Athena в Массачусетском технологическом университете в середине 80-х годов, и с тех пор этот протокол претерпел ряд принципиальных изменений, которые отразились в существующих ныне пяти версиях.

Kerberos разработан для сетей TCP/IP и построен на основе доверия участников протокола к третьей (доверенной) стороне. Служба Kerberos, работающая в сети, действует как доверенный посредник, обеспечивая надежную аутентификацию в сети с последующей авторизацией доступа клиента (клиентского приложения) к ресурсам сети. Защищенность установленных в рамках сессии Kerberos соединений обусловливается применением симметричных алгоритмов шифрования. Служба Kerberos разделяет отдельный секретный ключ с каждым субъектом сети, и знание такого секретного ключа равносильно доказательству подлинности субъекта сети.

Основу Kerberos составляет протокол аутентификации и распределения ключей Нидхэма — Шредера (Needham — Schroeder) с третьей доверенной стороной [7]. Рассмотрим эту версию протокола Нидхема — Шредера применительно к Kerberos. В протоколе Kerberos (версия 5) участвуют две взаимодействующие стороны и доверенный сервер KS, выполняющий роль центра распределения ключей KDC.

Вызывающий (исходный) объект обозначается через A, а вызываемый (объект назначения) — через B. Участники сеанса A и B имеют уникальные идентификаторы Id_A и Id_B соответственно. Стороны A и B, каждая по отдельности, разделяют свой секретный ключ с сервером KS.

Пусть сторона A хочет получить сеансовый ключ для информационного обмена со стороной B.

Сторона A инициирует фазу распределения ключей, посылая по сети серверу KS идентификаторы Id_A и Id_B:

(1) $A \rightarrow KS$: Id_A, Id_B.

Сервер KS генерирует сообщение с временной отметкой T, сроком действия L, случайным сеансовым ключом K и идентификатором Id_A.

Он шифрует это сообщение секретным ключом, который разделяет со стороной *B*.

Затем сервер *KS* берет временную отметку *T*, срок действия *L*, сеансовый ключ *K*, идентификатор Id_B стороны *B* и шифрует все это секретным ключом, который разделяет со стороной *A*. Оба эти зашифрованные сообщения он отправляет стороне *A*:

(2) $KS \rightarrow A$: $E_A(T, L, K, Id_B)$, $E_B(T, L, K, Id_A)$.

Сторона *A* расшифровывает первое сообщение своим секретным ключом, проверяет отметку времени *T*, чтобы убедиться, что это сообщение не является повторением предыдущей процедуры распределения ключей. Затем сторона *A* генерирует сообщение со своим идентификатором Id_A и отметкой времени *T*, шифрует его сеансовым ключом *K* и отправляет стороне *B*. Кроме того, *A* отправляет для *B* сообщение от *KS*, зашифрованное ключом стороны *B*:

(3) $A \rightarrow B$: $E_K(Id_A, T)$, $E_B(T, L, K, Id_A)$.

Только сторона *B* может расшифровать сообщения (3). Сторона *B* получает отметку времени *T*, срок действия *L*, сеансовый ключ *K* и идентификатор Id_A. Затем сторона *B* расшифровывает сеансовым ключом *K* вторую часть сообщения (3). Совпадение значений *T* и Id_A в двух частях сообщения подтверждают подлинность *A* по отношению к *B*.

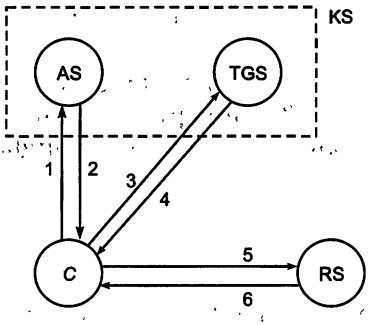
Для взаимного подтверждения подлинности сторона *B* создает сообщение, состоящее из отметки времени *T* плюс 1, шифрует его ключом *K* и отправляет стороне *A*:

(4) $B \rightarrow A$: $E_K(T + 1)$.

Если после расшифрования сообщения (4) сторона *A* получает ожидаемый результат, она знает, что на другом конце линии связи находится действительно *B*.

Этот протокол успешно работает при условии, что часы каждого участника синхронизированы с часами сервера *KS*. Следует отметить, что в этом протоколе необходим обмен с *KS* для получения сеансового ключа каждый раз, когда *A* желает установить связь с *B*. Протокол обеспечивает надежное соединение объектов *A* и *B* при условии, что ни один из ключей не скомпрометирован и сервер *KS* защищен.

Система Kerberos имеет структуру типа клиент/сервер и состоит из клиентских частей С, установленных на все рабочие станции пользователей и серверы сети, и сервера Kerberos KS, располагающегося на каком-либо (необязательно выделенном) компьютере (рис. 12.8). Клиентами могут быть пользователи, а также независимые программы, выполняющие такие действия, как загрузка удаленных файлов, отправка сообщений, доступ к базам данных, доступ к принтерам, получение привилегий у администратора и т. п.



Обозначения:

KS — сервер системы Kerberos
AS — сервер аутентификации
TGS — сервер службы выделения мандатов
RS — сервер информационных ресурсов
C — клиент системы Kerberos

Рис. 12.8. Схема работы протокола Kerberos

Сервер Kerberos KS, состоит из двух частей: сервера аутентификации AS (Authentication Server) и сервера службы выдачи мандатов TGS (Ticket Granting Service). Физически данные серверы могут быть совмещены. Информационными ресурсами, необходимыми клиентам C, управляет целевой сервер информационных ресурсов RS. Предполагается, что серверы службы Kerberos надежно защищены от физического доступа злоумышленников.

Сетевые службы, требующие проверки подлинности, и клиенты, которые хотят использовать эти службы, регистрируют в Kerberos свои секретные ключи. Kerberos хранит базу данных о клиентах и их секретных ключах. Наличие в этой базе данных секретных ключей каждого пользователя и ресурсов сети, поддерживающих данный протокол, позволяет создавать зашифрованные сообщения, направляемые клиенту или серверу; успешное расшифрование этих сообщений и является гарантией прохождения аутентификации всеми участниками протокола.

Kerberos также создает сеансовые ключи (Session Key), которые выдаются клиенту и серверу (или двум клиентам) и никому больше. Сеансовый ключ используется для шифрования сообщений, которыми обмениваются две стороны, и уничтожается после окончания сеанса.

Область действия системы Kerberos распространяется на тот участок сети, все пользователи которого зарегистрированы под своими именами и паролями в базе данных сервера Kerberos.

В общих чертах процесс идентификации и аутентификации пользователя в системе Kerberos версии 5 можно описать следующим образом (см. рис. 12.8).

Прежде всего следует отметить, что при использовании Kerberos нельзя напрямую получить доступ к целевому серверу информационных ресурсов RS.

Клиент C, желая получить доступ к информационным ресурсам сети, направляет запрос серверу аутентификации AS. Сервер AS идентифицирует пользователя с помощью его имени и пароля и высылает клиенту мандат (Ticket) на доступ к серверу службы выделения мандатов TGS (Ticket-Granting Service).

Для использования конкретного целевого сервера информационных ресурсов RS клиент C запрашивает у TGS мандат на обращение к

целевому серверу RS. Если все в порядке, TGS разрешает использование необходимых ресурсов сети и посылает соответствующий мандат клиенту C.

Основные шаги работы системы Kerberos (см. рис. 12.8):

1. C → AS — запрос клиента C к серверу AS разрешить обратиться к службе TGS.

2. AS → C — разрешение (мандат) от сервера AS клиенту C обратиться к службе TGS.

3. C → TGS — запрос клиента C к службе TGS на получение допуска (мандата) к серверу ресурсов RS.

4. TGS → C — разрешение (мандат) от службы TGS клиенту C для обращения к серверу ресурсов RS.

5. C → RS — запрос информационного ресурса (услуги) у сервера RS.

6. RS → C — подтверждение подлинности сервера RS и предоставление информационного ресурса (услуги) клиенту C.

Данная модель взаимодействия клиента с серверами может функционировать только при условии обеспечения конфиденциальности и целостности передаваемой управляющей информации. Без строгого обеспечения информационной безопасности клиент C не может отправлять серверам AS, TGS и RS свои запросы и получать разрешения на доступ к обслуживанию в сети.

Чтобы избежать возможности перехвата и несанкционированного использования информации, Kerberos применяет при передаче любой управляющей информации в сети систему многократного шифрования с использованием комплекса секретных ключей (секретный ключ клиента, секретный ключ сервера, секретные сеансовые ключи пары клиент/сервер). Kerberos может использовать различные симметричные алгоритмы шифрования и хэш-функции, однако обязательными для поддержки установлены алгоритм шифрования 3-DES или AES и хэш-функция MD5.

В системе Kerberos используется два типа верительных документов: мандат (Ticket) и аутентификатор (Authenticator).

Мандат используется для безопасной передачи серверу идентификационных данных клиента, которому выдан этот мандат. В нем также содержится информация, которую сервер может использовать для проверки того, что клиент, использующий мандат, — это именно тот клиент, которому данный мандат был выдан.

Аутентификатор — это дополнительный атрибут, предъявляемый вместе с мандатом.

В дальнейшем в этом разделе будет применяться система обозначений, используемая в документах Kerberos:

c — клиент;

s — сервер;

a — сетевой адрес клиента;

v — начало и окончание времени действия мандата;

t — метка времени;
K_x — секретный ключ x;
$K_{x,y}$ — сеансовый ключ для x и y;
$\{m\}K_x$ — сообщение m, шифрованное секретным ключом K_x субъекта x;
$T_{x,y}$ — мандат x на использование y;
$A_{x,y}$ — аутентификатор x для y.

Мандат Kerberos имеет следующую форму:

$$T_{c,s} = s, \{c, a, v, K_{c,s}\} K_s.$$

Мандат предоставляется одному клиенту для доступа к строго определенному серверу и на строго определенное время. Он содержит имя клиента, его сетевой адрес, начальное и конечное время действия клиента и сеансовый ключ $K_{c,s}$, зашифрованные на секретном ключе K_s сервера.

Если клиент получил мандат, он может использовать его для доступа к серверу в течение промежутка времени, отведенного для данного мандата. Клиент не может расшифровать мандат (он не знает секретного ключа K_s сервера), но он может предъявить его серверу в зашифрованной форме. Никто из подслушивающих в сети не сможет прочитать или изменить мандат при передаче его по сети.

Аутентификатор Kerberos имеет следующую форму:

$$A_{c,s} = \{c, t, \text{ключ}\}K_{c,s}.$$

Аутентификатор создается клиентом всякий раз, когда тот хочет получить доступ к целевому серверу. Аутентификатор содержит имя клиента, метку времени и сеансовый ключ, зашифрованные на сеансовом ключе $K_{c,s}$, общем для клиента и сервера.

В отличие от мандата, аутентификатор используется только один раз. Однако клиент может генерировать аутентификаторы по мере надобности (ему известен общий секретный ключ $K_{c,s}$). Использование аутентификатора преследует две цели. Во-первых, аутентификатор содержит некоторый открытый текст, зашифрованный сеансовым ключом. Это доказывает, что клиенту известен ключ. Во-вторых, зашифрованный открытый текст включает метку времени. Эта метка времени не позволяет злоумышленнику, перехватившему данный аутентификатор и мандат, использовать их спустя некоторое время для успешного прохождения процедуры аутентификации.

Сообщения Kerberos

В Kerberos версии 5 используется пять сообщений (см. рис. 12.8):

1. Клиент — Kerberos: c, tgs.
2. Kerberos — клиент: $\{K_{c,tgs}\} K_c \{T_{c,tgs}\} K_{tgs}$.
3. Клиент — TGS: $\{A_{c,s}\} K_{c,tgs} \{T_{c,tgs}\} K_{tgs,s}$.

4. TGS — клиент: $\{K_{c,s}\}\ K_{c,tgs}\ \{T_{c,s}\}\ K_s$.
5. Клиент — сервер: $\{A_{c,s}\}\ K_{c,s}\ \{T_{c,s}\}\ K_s$.

Рассмотрим использование этих сообщений подробнее.

Получение первоначального мандата

У клиента есть часть информации, доказывающей его личность, — его пароль. Понятно, что не следует заставлять клиента передавать пароль по сети. Протокол Kerberos минимизирует вероятность компрометации пароля, но при этом не позволяет пользователю правильно идентифицировать себя, если тот не знает пароль.

Клиент посылает на сервер аутентификации Kerberos сообщение, содержащее его имя и имя его сервера TGS:

Клиент — Kerberos: *c*, *tgs*.

В системе может быть несколько серверов TGS. На практике пользователь, скорее всего, просто вводит свое имя и программа входа в систему посылает запрос.

Сервер аутентификации Kerberos ищет данные о клиенте в своей базе данных. Если информация о клиенте есть в базе данных, Kerberos генерирует сеансовый ключ $K_{c,tgs}$, который будет использоваться для обмена данными между клиентом и TGS. Kerberos шифрует этот сеансовый ключ секретным ключом клиента K_c. Затем он создает для клиента *мандат на выделение мандата TGT (Ticket Granting Ticket)*, доказывающий службе TGS подлинность клиента. TGT зашифровывается на секретном ключе TGS и содержит идентификаторы клиента и сервера, сеансовый ключ пары TGS/клиент, а также начальное и конечное время действия TGT. Сервер аутентификации посылает клиенту эти два зашифрованных сообщения:

Kerberos — клиент: $\{K_{c,tgs}\}\ K_c\ \{T_{c,tgs}\}\ K_{tgs}$.

Теперь клиент принимает данные сообщения, расшифровывает первое сообщение своим секретным ключом K_c и получает сеансовый ключ $K_{c,tgs}$. Секретный ключ является однонаправленной хэш-функцией клиентского пароля, поэтому у законного пользователя не будет никаких проблем. Злоумышленник не знает правильного пароля и, следовательно, не может расшифровать ответ сервера аутентификации. Поэтому злоумышленник не может получить мандат или сеансовый ключ.

Клиент сохраняет мандат TGT и сеансовый ключ, стирая пароль и хэш-значение. Эта информация уничтожается для уменьшения вероятности компрометации. Если злоумышленник попытается скопировать память клиента, он получит только TGT и сеансовый ключ. Эти данные важны, но лишь на время жизни TGT. Когда срок действия TGT истечет, эти сведения станут бессмысленными. Теперь клиент имеет

возможность пройти аутентификацию у TGS-сервера при помощи полученного мандата TGT в течение всего срока действия TGT, указанного в нем.

Получение серверных мандатов

Далее клиент может получить отдельный мандат для каждой нужной ему услуги. С этой целью клиент должен послать в службу TGS запрос:

Клиент — TGS: $\{A_{c,s}\}\ K_{c,tgs}\ \{T_{c,tgs}\}\ K_{tgs,s}$.

На практике программное обеспечение посылает запрос автоматически, т. е. невидимо для пользователя. Этот запрос состоит из мандата TGT и аутентификатора. Аутентификатор, зашифрованный на ключе парной связи клиента и сервера TGS, содержит идентификаторы клиента и требующегося ему сервера, случайный сеансовый ключ и метку времени.

TGS, получив запрос, расшифровывает TGT своим секретным ключом. Затем TGS использует включенный в TGT сеансовый ключ, чтобы расшифровать аутентификатор. В завершение производится сравнение информации, содержащейся в аутентификаторе, с информацией мандата. Точнее, сетевой адрес клиента в мандате сличается с сетевым адресом, указанным в запросе, а также сравнивается метка времени с текущим временем. Если все совпадает, TGS разрешает выполнение запроса. Если время, указанное в запросе, значительно отличается от текущего момента, TGS считает такой запрос попыткой повторения предыдущего запроса.

Служба TGS должна также отслеживать правильность сроков действия аутентификаторов, так как услуги сервера могут запрашиваться несколько раз последовательно с одним мандатом, но разными аутентификаторами. Другой запрос с тем же мандатом и уже использованной меткой времени аутентификатора будет отвергнут.

В ответ на верный запрос TGS предоставляет клиенту мандат для доступа к целевому серверу. TGS также создает сеансовый ключ для клиента и целевого сервера, зашифрованный сеансовым ключом, общим для клиента и TGS. Оба этих сообщения отправляются клиенту:

TGS — клиент: $\{K_{c,s}\}\ K_{c,tgs}\{T_{c,s}\}\ K_s$.

Клиент расшифровывает сообщение и извлекает сеансовый ключ.

Запрос услуги

Теперь клиент может доказать свою подлинность целевому серверу. Для успешного прохождения аутентификации у целевого сервера клиент создает аутентификатор, состоящий из его имени, сетевого адреса и

метки времени и зашифрованный на сеансовом ключе «клиент/сервер», и отправляет его вместе с мандатом, зашифрованным на секретном ключе целевого сервера, который был передан от службы TGS:

Клиент — сервер: $\{A_{c,s}\}\ K_{c,s}\ \{T_{c,s}\}\ K_s$.

Приняв данные от клиента, целевой сервер проводит проверку аутентификатора. Он расшифровывает его при помощи своего секретного ключа и извлекает из него сеансовый ключ «клиент/сервер». Мандат также подвергается проверке. Процедура проверки схожа с процедурой, проводимой в случае сессии клиент — TGS, т. е. проверяется соответствие сетевых адресов и временной метки. Если все в порядке, то сервер уверен, что клиент — именно тот, за кого он себя выдает.

Если приложение требует взаимной проверки подлинности, сервер посылает клиенту сообщение, состоящее из метки времени, зашифрованной сеансовым ключом. Это доказывает, что серверу известен правильный секретный ключ и он может расшифровать мандат и удостоверение. При необходимости клиент и сервер могут шифровать дальнейшие сообщения общим ключом. Так как этот ключ известен только им, они оба могут быть уверены, что последнее сообщение, зашифрованное этим ключом, отправлено другой стороной. На практике вся эта сложная процедура аутентификации производится автоматически.

Kerberos может использоваться и для междоменной аутентификации. В случае обращения клиента в центр распределения ключей KDC (Key Distribution Center) для доступа к серверу, находящемуся в другом домене, KDC выдает клиенту *мандат переадресации (Refferal Ticket)* для обращения к KDC того домена, в котором находится требуемый сервер.

Следует помнить, что Kerberos, как и любое другое программное средство криптографической защиты, работает в недоверенной программной среде. Безопасность Kerberos во многом зависит от надежности защиты рабочей станции, на которой установлен данный протокол.

К самому протоколу Kerberos предъявляется ряд дополнительных требований, которые подробно описаны в RFC-1510. Приведем только основные из них:

- службы Kerberos должны быть защищены от атак, направленных на отказ в обслуживании;
- необходима синхронизация системного времени всех участников системы, поскольку метки времени участвуют в процессе аутентификации;
- Kerberos не защищает от атак подбором пароля. Проблема в том, что хранящийся в KDC ключ пользователя является результатом переработки его пароля с помощью хэш-функции. В случае слабого пароля возможен его подбор;
- службы Kerberos должны быть надежно защищены от всех видов несанкционированного доступа;
- полученные клиентом мандаты, а также секретные ключи должны быть защищены от несанкционированного доступа.

Невыполнение указанных требований может стать причиной успешной атаки.

На сегодня протокол Kerberos является широко распространенным средством аутентификации. Kerberos может использоваться в сочетании с различными криптографическими схемами, включая шифрование с открытым ключом.

Вопросы для самоконтроля

1. Что представляет собой список контроля доступа ACL?
2. Охарактеризуйте основные методы управления удаленным доступом.
3. Опишите функционирование системы управления сетевым доступом.
4. Укажите особенности системы управления веб-доступом.
5. Назовите и охарактеризуйте средства и протоколы аутентификации удаленных пользователей.
6. Как осуществляется аутентификация на основе одноразовых паролей OTP?
7. Дайте сравнительную характеристику протоколов PAP, CHAP и EAP.
8. Каковы назначение и особенности функционирования протокола S/Key?
9. Опишите работу протокола централизованного контроля доступа к сети TACACS.
10. Укажите отличия системы централизованного контроля доступа к сети RADIUS от системы TACACS.
11. Опишите работу протокола аутентификации и распределения ключей Нидхэма — Шредера с участием доверенного сервера KS, выполняющего роль центра распределения ключей KDC.
12. Опишите назначение и функционирование протокола Kerberos.

Глава 13
ОБНАРУЖЕНИЕ И ПРЕДОТВРАЩЕНИЕ ВТОРЖЕНИЙ

Системы предотвращения вторжений IPS (Intrusion Prevention System) предназначены обеспечить безопасность защищаемых объектов от воздействия, которое признано вторжением в КИС.

Раньше на периметре сети устанавливали всего два класса защитных средств — межсетевые экраны и системы обнаружения вторжений IDS. Межсетевые экраны (МЭ) пропускали трафик через себя, но не «заглядывали» внутрь пересылаемых данных, анализируя только заголовки IP-пакетов. Системы IDS напротив, анализировали то, что упускалось из виду межсетевыми экранами, но не были способны блокировать атаки, так как трафик через них не проходил. На стыке этих двух технологий родился новый класс защитных средств — системы предотвращения вторжений IPS.

Системы IPS оказались настолько популярными, что некоторые производители стали рекламировать свои IDS как системы предотвращения атак, т. е. IPS, тем самым незаслуженно открывая для себя новые рынки и новых клиентов.

На самом деле системы предотвращения вторжений IPS существенно превосходят по своим возможностям системы обнаружения вторжений IDS. Системы IPS объединяют целый ряд технологий безопасности и достаточно далеко продвинулись по сравнению со своими предшественниками — системами обнаружения вторжений IDS.

13.1. Основные понятия

Обнаружение вторжений — это процесс мониторинга событий, происходящих в информационной системе и их анализа на наличие признаков, указывающих на попытки вторжения: нарушения конфиденциальности, целостности, доступности информации или политики информационной безопасности.

Предотвращение вторжений — процесс блокировки выявленных вторжений.

Средства системы обнаружения и предотвращения вторжений IPS автоматизируют данные процессы и необходимы в организации любого

уровня, чтобы предотвратить ущерб и потери, к которым могут привести вторжения.

В отличие от системы IDS признаками настоящей системы IPS являются следующие:

- система IPS функционирует в режиме inline (пропускает трафик через себя) на скорости канала. Иначе говоря, решение IPS не снижает скорость передачи данных;
- система IPS обеспечивает сборку передаваемых пакетов в правильном порядке и анализирует эти пакеты с целью обнаружения следов несанкционированной активности;
- во время анализа используются различные методы обнаружения атак — сигнатурный и поведенческий, — а также идентификация аномалий в протоколах;
- система IPS в состоянии блокировать вредоносный трафик.

Таким образом, чтобы получить систему IPS из IDS, надо не только заменить одну букву в названии, но и изменить принципы работы решения, добавив новые технологии.

При рассмотрении IPS применяют классификацию, унаследованную от систем обнаружения вторжений — деление средств предотвращения вторжений на сетевые и хостовые.

Сетевая система NIPS (Network-based IPS) представляет средство предотвращения вторжений сетевого уровня, которое находится на пути передачи сетевого трафика и осуществляет его мониторинг. Основная задача сетевой NIPS — защита группы хостов сети от возможных атак путем анализа передаваемого трафика и блокирования трафика, связанного с проведением атак.

Хостовая система HIPS (Host-based IPS) — это средство предотвращения вторжений уровня хоста, которое располагается на конкретном хосте и обеспечивает его защиту от разрушающих воздействий путем анализа сетевого трафика, поведения приложений, активируемых системных вызовов и т. п.

В системе предотвращения вторжений IPS выделяют также средства защиты от распределенных атак типа «отказ в обслуживании».

Во многих средствах защиты сегодня объединены возможности обнаружения и блокирования вторжений, поэтому иногда их условно называют продуктами IDS/IPS.

Однако для эффективной защиты применения только средств IPS оказывается недостаточно — желательно знать заранее слабые места (уязвимости) КИС, называемые в обиходе дырами, через которые злоумышленники могут успешно осуществить атаку. Дырами могут стать слабые пароли, несоответствия в настройках сетевых устройств, уязвимости операционных систем и приложений и т. п.

Для поиска и выявления таких уязвимостей существуют специализированные средства — *сканеры уязвимости (Vulnerability Assessment)*. Их использование в КИС существенно повышает уровень защиты: определив слабые места, администратор безопасности может предпринять соответствующие меры по их устранению до того, как злоумышленник

воспользуется ими. В последнее время стали появляться специализированные средства, которые обеспечивают автоматический процесс устранения уязвимостей, но пока подобные решения предлагают немногие производители.

Чтобы максимально снизить риск негативного воздействия атак, необходимо объединить средства IPS, сканеры уязвимости и средства устранения уязвимостей в единую подсистему с централизованным управлением.

Решение по предотвращению вторжений состоит из сенсоров, одного или нескольких серверов управления, сканеров уязвимости, средств устранения уязвимостей, консоли оператора и администраторов (рис. 13.1) [3]. Иногда выделяется внешняя база данных для хранения информации о событиях информационной безопасности и их параметров.

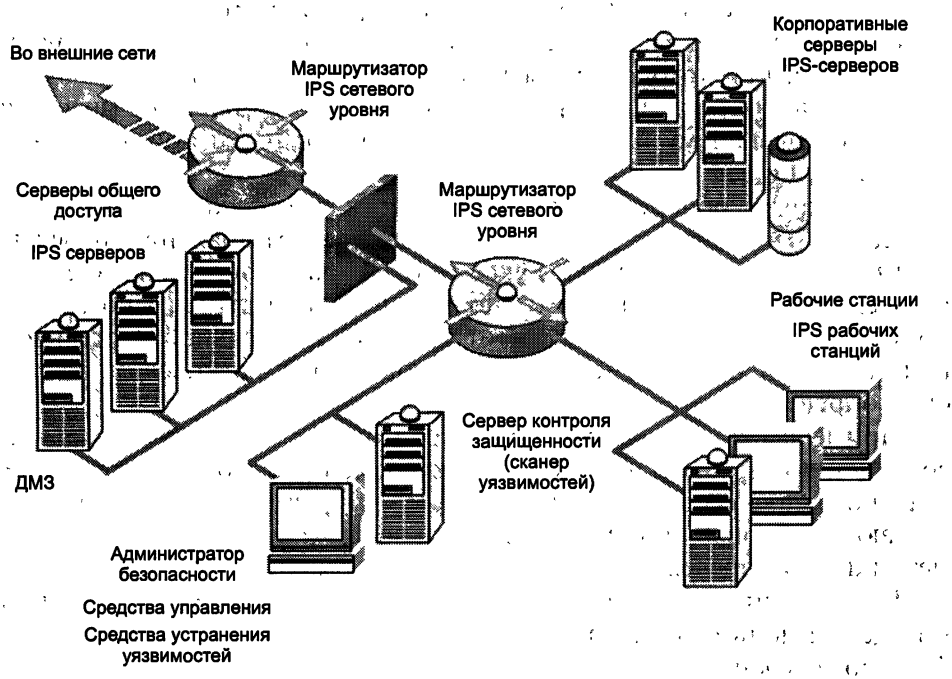


Рис. 13.1. Подсистема предотвращения вторжений в КИС

Сканеры уязвимости осуществляют поиск и выявление уязвимостей в КИС. Сервер управления получает информацию от сенсоров обнаружения атак и управляет ими. Обычно на серверах осуществляется консолидация и корреляция событий. Для более глубокой обработки важных событий средства предотвращения вторжений системного уровня интегрируются с подсистемой мониторинга и управления инцидентами.

Консоли представляют интерфейсы для операторов и администраторов подсистемы. Обычно это программное средство, устанавливаемое

на рабочей станции. Для организации централизованного администрирования, управления обновлениями сигнатур, управления конфигурациями применяется интеграция с подсистемой управления средствами защиты организации.

Необходимо учитывать, что только комплексное использование разных типов средств подсистемы позволяет достигнуть всестороннего и точного обнаружения и предотвращения вторжений.

13.2. Обнаружение вторжений системой IPS

В процессе выявления вторжений используются следующие методы анализа событий:

- обнаружение аномального поведения (Anomaly-based), при котором определяются аномальные (ненормальные) события;
- обнаружение злоупотреблений (Misuse Detection или Signature-based), при котором событие или множество событий проверяются на соответствие заранее определенному образцу (шаблону), описывающему известную атаку. Шаблон известной атаки называется сигнатурой [36].

Технология обнаружения атак путем идентификации *аномального поведения* основана на следующей гипотезе. Аномальное поведение пользователя (т. е. атака или какое-нибудь враждебное действие) часто проявляется как отклонение от нормального поведения. События при попытке вторжения отличаются от событий нормальной деятельности пользователей или взаимодействия узлов сети и могут, следовательно, быть определены.

Примером аномального поведения может служить большое число соединений за короткий промежуток времени, высокая загрузка центрального процессора и т. п. Сенсоры собирают данные о событиях, создают шаблоны нормальной деятельности и используют различные метрики для определения отклонения от нормального состояния.

Если можно было бы однозначно описать профиль нормального поведения пользователя, то любое отклонение от него можно идентифицировать как аномальное поведение. Однако аномальное поведение не всегда является атакой. Например, одновременную посылку большого числа запросов от администратора сети подсистема обнаружения атак может идентифицировать как атаку типа «отказ в обслуживании».

При использовании такой технологии возможны два крайних случая:

- обнаружение аномального поведения, которое не является атакой, и отнесение его к классу атак;
- пропуск атаки, которая не подпадает под определение аномального поведения.

Второй случай более опасен, чем ложное отнесение аномального поведения к классу атак.

При настройке и эксплуатации систем этой категории администраторы сталкиваются со следующими проблемами:

- построение профиля пользователя является трудно формализуемой и трудоемкой задачей, требующей от администратора большой предварительной работы;
- определение граничных значений характеристик поведения пользователя для снижения вероятности появления одного из двух вышеназванных крайних случаев.

Технология обнаружения аномалий ориентирована на выявление новых типов атак. Однако ее недостаток — необходимость постоянного обучения. Пока технология обнаружения аномалий не получила широкого распространения. Связано это с тем, что данная технология трудно реализуема на практике. Однако сейчас наметился определенный интерес к ней.

Суть другого подхода к обнаружению атак — *обнаружение злоупотреблений* — заключается в описании атаки в виде сигнатуры (Signature) и поиска данной сигнатуры в контролируемом пространстве (сетевом трафике или журнале регистрации).

В качестве сигнатуры атаки может выступать шаблон действий или строка символов, характеризующие аномальную деятельность. Эти сигнатуры хранятся в базе данных, аналогичной той, которая используется в антивирусных системах. Следует заметить, что антивирусные резидентные мониторы являются частным случаем подсистемы обнаружения атак, но поскольку эти направления изначально развивались параллельно, то принято разделять их. Поэтому данная технология обнаружения атак очень похожа на технологию обнаружения вирусов, при этом система может обнаружить все известные атаки. Однако системы данного типа не могут обнаруживать новые, еще не известные виды атак.

Подход, реализованный в таких системах, достаточно прост, и именно на нем основаны практически все системы обнаружения атак.

Однако при эксплуатации и этих систем администраторы сталкиваются с проблемами. Первая проблема заключается в создании механизма описания сигнатур, т. е. языка описания атак. Вторая проблема, связанная с первой, заключается в том, как описать атаку, чтобы зафиксировать все возможные ее модификации.

Следует отметить, что для достоверного обнаружения факта вторжения недостаточно найти некий характерный шаблон трафика, или сигнатуру. Для успешного обнаружения вторжений современная IPS должна обладать следующими свойствами и функциями:

- использовать знания о топологии защищаемой сети;
- проводить анализ сеанса взаимодействия с учетом протоколов, используемых для передачи данных;
- выполнять восстановление фрагментированных IP-пакетов до их анализа, не передавать фрагменты IP-дейтаграмм без проверки;
- отслеживать попытки создания перекрывающихся фрагментов IP-дейтаграмм, попытки перезаписи содержимого TCP-сегментов и предотвращать их;

- обеспечивать проверку соответствия логики/форматов работы по протоколу соответствующим RFC;
- выполнять статистический анализ данных;
- поддерживать механизмы сигнатурного поиска;
- обладать возможностью обучения и самообучения.

Кроме того, поскольку IPS может принимать решения о блокировании трафика, необходимо обеспечить надежное и безопасное удаленное управление IPS.

Средства конфигурирования IPS должны быть удобны для конечных пользователей. Большинство IPS поддерживают возможность задания пользовательских правил обнаружения вторжений для возможности подстройки IPS под конкретную среду или требования конкретного заказчика.

13.3. Предотвращение вторжений в КИС

Система обнаружения и предотвращения вторжений IPS охватывает решения следующих задач:

- предотвращение вторжений системного (хостового) уровня;
- предотвращение вторжений сетевого уровня;
- защита от DDoS-атак.

Предотвращение вторжений системного уровня

Средства предотвращения вторжений системного (хостового) уровня HIPS (Host-based IPS) действуют на уровне информационных узлов. Подсистема HIPS обеспечивает незамедлительное блокирование атак системного уровня и оповещение ответственных лиц.

Агенты (локальные сенсоры) обнаружения атак системного уровня собирают информацию, отражающую деятельность, которая происходит в отдельном информационном узле. Средства HIPS анализируют файлы журнала и ведут мониторинг пользовательской, сетевой и системной активности на узле информационной системы.

Логически локальные сенсоры устанавливаются между ядром ОС и пользовательским приложением. Локальные сенсоры перехватывают вызовы, обращенные к системе, сопоставляют их с правилами доступа, определенными политикой безопасности, и затем разрешают или запрещают доступ к ресурсам. Некоторые локальные сенсоры сличают запросы с БД известных сигнатур атак или аномального поведения.

Преимуществами данной подсистемы являются возможность контроля доступа к информационным объектам узла, проверка их целостности, регистрация аномальной деятельности конкретного пользователя.

К недостаткам можно отнести невозможность обнаружения комплексных аномальных событий, необходимость установки средств HIPS

на все защищаемые узлы. Кроме того, уязвимости операционной системы могут нарушить целостность и работу сенсоров.

Средства предотвращения вторжений системного (хостового) уровня HIPS могут быть установлены на рабочей станции или сервере. При этом IPS уровня хоста реализуется несколькими способами:

- в виде программного обеспечения, интегрированного в операционную систему. Пока все решения ограничиваются ОС семейства UNIX;
- в виде прикладного ПО, устанавливаемого на рабочей станции или сервере поверх операционной системы. Выпускается многими производителями: Cisco Systems, ISS, McAfee, Star Force и др. Кроме отражения сетевых атак, такие IPS обладают еще большим количеством полезных функций: контроль доступа к USB, создание замкнутой программной среды, контроль утечки информации, контроль загрузки с посторонних носителей и т. д.;
- система IPS может представлять собой отдельную подсистему отражения атак, реализованную в сетевой карте. Некоторые производители (в частности, D-Link) выпускают такого рода устройства, однако их распространенность невелика [36].

Предотвращение вторжений сетевого уровня

Подсистема предотвращения вторжений сетевого уровня NIPS (Network-based IPS) обеспечивает немедленное блокирование сетевых атак и оповещение ответственных лиц. Преимуществом применения средств сетевого уровня является возможность защиты одним средством сразу нескольких узлов или сегментов сети.

Программные или программно-аппаратные средства Network IPS (сетевые сенсоры) анализируют сетевой трафик определенных узлов или сегментов сети, а также сетевые, транспортные и прикладные протоколы взаимодействия.

Для обнаружения вторжения используется либо сравнение битной последовательности проходящего потока данных с эталонным образцом (сигнатурой) атаки, либо фиксация подозрительной (аномальной) сетевой активности посредством анализа сетевого трафика или нарушений правил политики безопасности. В случае обнаружения попыток атаки применяются меры противодействия.

В качестве мер противодействия могут выполняться:

- блокирование выбранных сетевых пакетов;
- изменение конфигурации средств других подсистем обеспечения информационной безопасности (например, межсетевого экрана) для более эффективного предотвращения вторжения;
- сохранение выбранных пакетов для последующего анализа;
- регистрация событий и оповещение ответственных лиц.

Дополнительной возможностью данных средств является сбор информации о защищаемых узлах. Для получения информации о защи-

щенности и критичности узла или сегмента сети применяется интеграция с подсистемой контроля эффективности защиты информации.

IPS сетевого уровня могут быть реализованы как:

- выделенные аппаратные устройства (Security Appliance), которые могут быть установлены на периметре корпоративной сети и в ряде случаев внутри нее. Такие устройства — наиболее распространенный вариант. Основными производителями таких средств являются компании Cisco Systems, ISS, Juniper, 3Com, McAfee и др.;
- решения, интегрированные в инфраструктуру корпоративной сети.

Решения, интегрированные в инфраструктуру, гораздо эффективнее выделенных аппаратных устройств:

- стоимость интегрированного решения ниже стоимости автономного (Stand-alone) устройства;
- ниже и стоимость внедрения (финансовая и временная) такого решения — можно не менять топологию сети;
- надежность выше, так как в цепочке прохождения трафика отсутствует дополнительное звено, подверженное отказам;
- интегрированные решения предоставляют более высокий уровень защиты за счет более тесного взаимодействия с защищаемыми ресурсами.

Сама интеграция может быть выполнена различными путями:

- *использование маршрутизатора (Router)* — самый распространенный способ. В этом случае система IPS становится составной частью данного устройства и получает доступ к анализируемому трафику сразу после поступления его на определенный интерфейс. Система IPS может быть реализована в виде отдельного модуля, вставляемого в шасси маршрутизатора, или как неотъемлемая часть операционной системы маршрутизатора. Первой в данном направлении развития систем IPS стала компания Cisco Systems. Однако система IPS, интегрированная в маршрутизатор, умеет отражать атаки только на периметре сети, оставляя внутренние ресурсы без защиты;
- *использование коммутаторов локальной сети (Switch)*, в которые могут быть внедрены механизмы предотвращения атак, причем как в составе ОС, так и в виде отдельного аппаратного модуля. Эту технологию интеграции IPS в коммутаторы реализовала Cisco Systems в своем семействе Cisco Catalyst;
- *использование точек беспроводного доступа (Wireless Access Point)*, через которые может проходить трафик, нуждающийся в анализе. По пути интеграции пошли такие производители, как Cisco Systems и Aruba, оснастившие свое оборудование необходимыми функциями. Такие системы, помимо обнаружения и предотвращения различных атак, умеют определять местонахождение несанкционированно установленных беспроводных точек доступа и клиентов [36].

Пример схемы предотвращения вторжений сетевого уровня на основе продуктов Cisco Systems приведен на рис. 13.2 [98].

Сравнительная характеристика подсистем Network IPS и Host IPS приведена в табл. 13.1 [3].

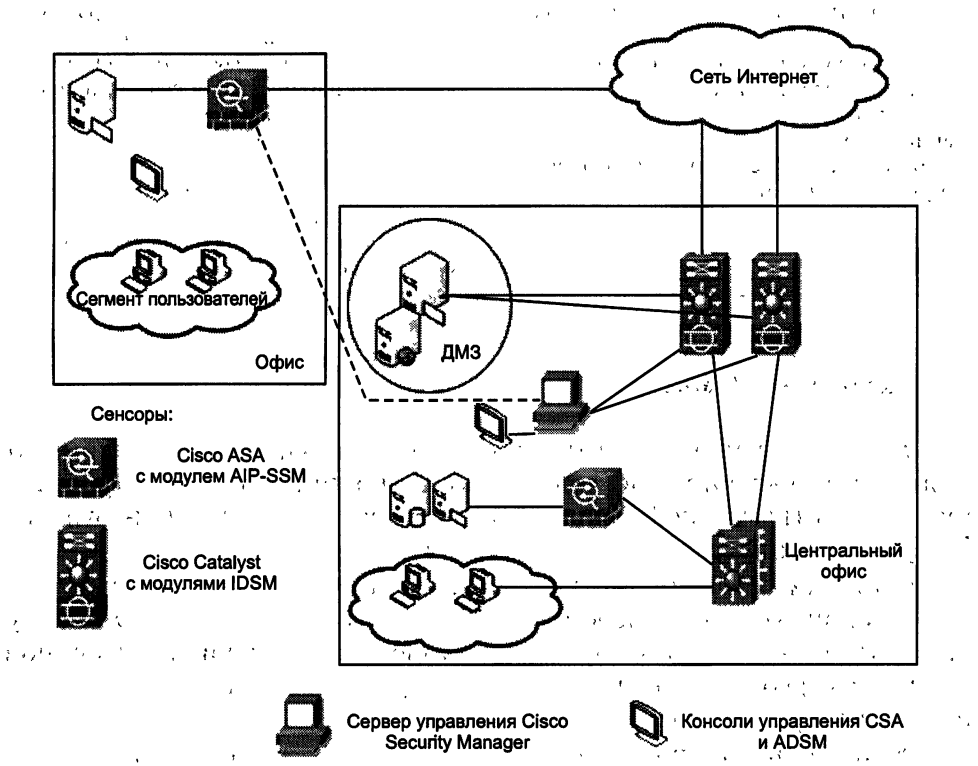


Рис. 13.2. Схема предотвращения вторжений сетевого уровня на основе продуктов компании Cisco Systems

Таблица 13.1. **Сравнительная характеристика подсистем Network IPS и Host IPS**

Достоинства	Недостатки
Network IPS	
Широта применения — целая сеть может быть покрыта одним сетевым сенсором. Минимальные неудобства от установки обновлений сигнатур и обновлений ПО сенсоров. Предотвращение DoS-атаки. Возможность обнаружения ошибок сетевого уровня в стеке TCP/IP. Независимость от ОС информационных узлов	Наряду с верными бывают и ложные срабатывания. Не может анализировать зашифрованный поток данных. Новые виды или варианты атак не будут выявлены в случае отсутствия сигнатуры данной атаки. Задержка во времени между моментом обнаружения атаки и моментом оповещения (тревоги). Затруднен анализ пакетов в случае перегруженной сети. Отсутствуют уведомления об успешности атаки

Окончание табл. 13.1

Достоинства	Недостатки
Host IPS	
Возможность связывать пользователя с событием. Может обнаруживать атаки, не зафиксированные сенсорами NIDS. Может проводить анализ данных, расшифрованных на узле. Возможность предоставления информации об узле в течение атаки на него	Для защиты нескольких узлов сенсоры должны быть установлены на каждом из них. Если ОС взломана в результате атаки, то перестает функционировать и сенсор, установленный на данном узле. Сенсор не способен обнаруживать деятельность сетевых сканеров. Сенсоры могут быть неэффективными в случае DoS-атаки на узел. Для функционирования необходимы дополнительные ресурсы

Защита от DDoS-атак

Одним из наиболее критичных по последствиям классов компьютерных атак являются распределенные атаки типа «отказ в обслуживании» DDoS (Distributed Denial of Service), направленные на нарушение доступности информационных ресурсов.

Эти атаки осуществляются с использованием множества программных компонентов, размещаемых на хостах в сети Интернет. Они могут привести не только к выходу из строя отдельных узлов и сервисов, но и остановить работу корневых DNS-серверов и вызвать частичное или полное прекращение функционирования сети.

Основная цель защиты против DDoS-атак заключается в предотвращении их реализации, точном обнаружении этих атак и быстром реагировании на них. При этом важно также эффективно распознавать легитимный трафик, который имеет признаки, схожие с трафиком вторжения, и обеспечивать надежную доставку легитимного трафика по назначению.

Общий подход к защите от атак DDoS включает реализацию следующих механизмов:

- обнаружение вторжения;
- определение источника вторжения;
- предотвращение вторжения.

Система защиты предприятий от DDoS-атак. При разработке данного решения необходим комплексный подход для построения системы защиты, способной защитить не только отдельные серверы предприятия, но и каналы связи с соответствующими операторами связи. Решение представляет собой многоуровневую систему с четко выстроенной линией обороны. Внедрение решения позволяет повысить защищенность корпоративной сети, устройств маршрутизации, канала связи, почтовых, веб- и DNS-серверов.

Внедрение такой системы защиты целесообразно в следующих случаях:

- осуществление компаниями своего бизнеса через Интернет;
- наличие корпоративного веб-сайта компании;
- использование сети Интернет для реализации бизнес-процессов.

Схема защиты предприятия от DDoS-атак представлена на рис. 13.3.

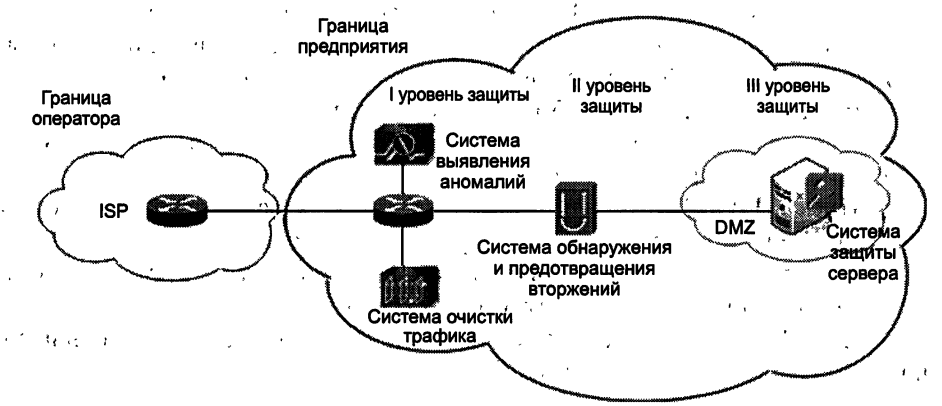


Рис. 13.3. Схема защиты предприятий от DDoS-атак

В данном решении применяются сенсоры обнаружения аномалий, просматривающие проходящий внешний трафик в непрерывном режиме. Данная система находится на границе с оператором связи, таким образом, процесс очистки начинается еще до попадания трафика атаки во внутреннюю сеть компании.

Метод обнаружения аномалий не может обеспечить 100-процентную вероятность очистки трафика, поэтому появляется необходимость интеграции с подсистемами предотвращения атак на сетевом и системном уровнях.

Кроме того, при реализации данного решения необходимо принять меры дополнительной безопасности, позволяющие укрепить сеть оператора связи и подготовить ее для быстрого противодействия и максимальной защиты от сетевых угроз различных видов.

Решение для операторов связи по обнаружению и подавлению DDoS-атак. Данное решение позволяет операторам связи предложить своим клиентам защиту от распределенных DDoS-атак и одновременно укрепить и защитить собственные сети. Фундаментальной задачей решения является удаление аномального трафика из канала связи и доставка только легитимного трафика.

Бизнес-преимущества внедряемого решения:

- возможность предложить новый сервис высокого уровня с перспективой масштабирования для больших, средних и малых предприятий;
- возможность позиционировать себя как доверенное лицо, участвующее в предотвращении ущерба и потерь клиентов;

- улучшение управляемости сетевой инфраструктурой;
- возможность предоставления абонентам отчетов об атаках.

Провайдер услуг может предлагать защиту от DDoS-атак своим корпоративным клиентам по двум схемам:

- *выделенная услуга* — подходит для компаний, бизнес которых связан с сетью Интернет: это компании, занимающиеся онлайновой торговлей, финансовые структуры и другие предприятия электронной коммерции. Выделенная услуга обеспечивает возможность очистки передаваемого трафика, а также дополнительные возможности обнаружения DDoS-атак и активацию процедур очистки трафика по требованию клиента;
- *услуга коллективного пользования* — предназначена для корпоративных клиентов, которым необходим определенный уровень защиты от DDoS-атак для своих онлайновых сервисов. Однако эта проблема не стоит для них остро. Услуга предлагает возможность очистки трафика коллективно для всех клиентов и стандартную политику для обнаружения DDoS-атаки.

На рис. 13.4 показана архитектура решения для операторов связи по обнаружению и подавлению DDoS-атак [98].

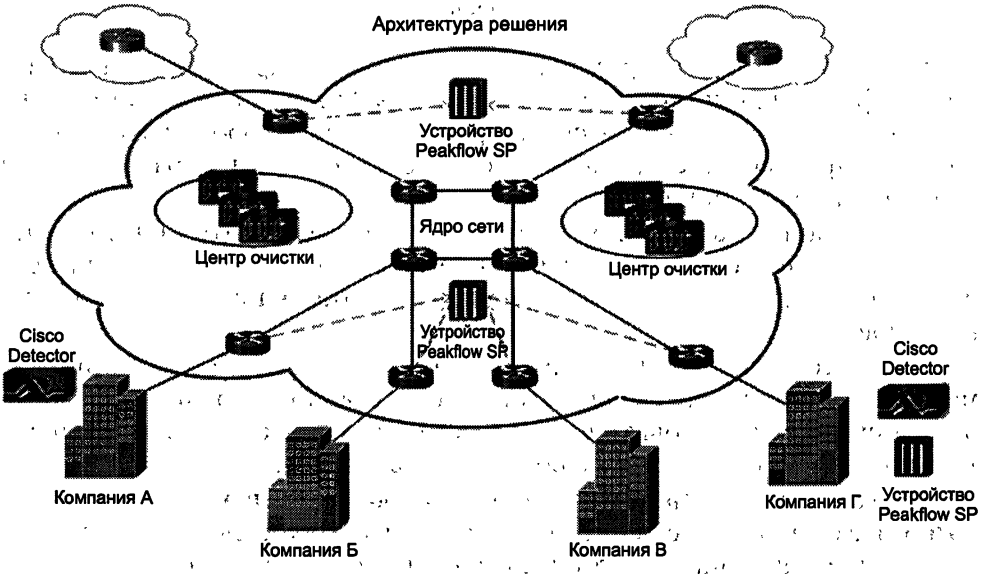


Рис. 13.4. Архитектура решения для операторов связи по обнаружению и подавлению DDoS-атак

Архитектура решения предлагает упорядоченный подход к обнаружению распределенных DDoS-атак, отслеживанию их источника и их подавлению.

В начале своей работы средствам защиты от DDoS-атак необходимо пройти процесс обучения и создать модель нормального поведения трафика в пределах сети, используя поток данных, доступный с маршрутизаторов.

После обучения система переходит в режим мониторинга трафика, и в случае обнаружения аномальной ситуации системному администратору отправляется уведомление. Если атака подтверждается, администратор безопасности сети переводит устройство очистки трафика в режим защиты.

Также возможно настроить устройства мониторинга на автоматическую активацию средств очистки трафика в случае обнаружения аномального трафика. При включении режима защиты средство фильтрации изменяет таблицу маршрутизации граничного маршрутизатора с целью перенаправления входящего трафика на себя и производит его очистку. После этого очищенный трафик перенаправляется в сеть.

Достоинства данного решения:

- мгновенная реакция на DDoS-атаки;
- возможность включения системы только по требованию обеспечивает максимальную надежность и минимальные затраты на масштабирование.

Вопросы для самоконтроля

1. Сформулируйте понятия «обнаружение вторжений» и «предотвращение вторжений».
2. Укажите четыре признака системы IPS, отличающих ее от системы IDS.
3. Дайте определения понятий «сетевая система NIPS» и «хостовая система HIPS».
4. Опишите назначение и особенности применения специализированных средств — сканеров уязвимости.
5. Какие методы анализа событий используются в процессе выявления вторжений?
6. В чем заключается метод обнаружения аномального поведения?
7. В чем заключается метод обнаружения злоупотреблений?
8. Опишите функциональность средств предотвращения вторжений системного (хостового) уровня HIPS.
9. Опишите функциональность средств предотвращения вторжений сетевого уровня NIPS.
10. Расскажите о подходе к защите от распределенных атак типа «отказ в обслуживании».
11. Какими свойствами и функциями должна обладать современная IPS для успешного обнаружения и предотвращения вторжений?
12. Опишите структуру и функционирование подсистемы предотвращения вторжений в КИС.

Глава 14
ЗАЩИТА ОТ ВРЕДОНОСНЫХ ПРОГРАММ И СПАМА

Существуют программы, намеренно написанные с целью уничтожения данных на чужом компьютере, похищения чужой информации, несанкционированного использования чужих ресурсов. Такие программы несут вредоносную нагрузку и соответственно называются вредоносными.

14.1. Классификация вредоносных программ

Вредоносные программы классифицируют по способу проникновения, размножения и типу вредоносной нагрузки.

В соответствии со способами распространения и вредоносной нагрузки все вредоносные программы можно разделить на четыре основных типа: компьютерные вирусы, черви, трояны и другие программы.

Следует отметить, что компьютерным вирусом часто называют любую вредоносную программу. Это обусловлено тем, что первые известные вредоносные программы были именно компьютерными вирусами и в течение последующих десятилетий число вирусов значительно превышало количество всех остальных вредоносных программ. Однако в последнее время наметились тенденции к появлению новых, невирусных технологий, которые используют вредоносные программы. При этом доля истинных вирусов в общем числе инцидентов с вредоносными программами за последние годы значительно сократилась.

В настоящее время вредоносные программы — это уже большей частью именно не вирусы, хотя такие термины, как «вирус» и «заражение вирусом», применяются по отношению ко всем вредоносным программам. Поэтому далее под термином «вирус» будет пониматься и вредоносная программа.

Компьютерные вирусы

Компьютерный вирус — это программа, способная создавать свои дубликаты и внедрять их в компьютерные сети и/или файлы, системные области компьютера и прочие выполняемые объекты. При этом дубликаты сохраняют способность к дальнейшему распространению.

Основная цель любого компьютерного вируса — это распространение на другие ресурсы компьютера и выполнение специальных действий при определенных событиях или действиях пользователя (например, 26-го числа каждого четного месяца или при перезагрузке компьютера). Специальные действия нередко оказываются вредоносными.

Жизненный цикл любого компьютерного вируса можно разделить на четыре этапа:

- проникновение на чужой компьютер;
- активация;
- поиск объектов для заражения;
- подготовка и внедрение копий.

Путями проникновения вируса могут служить как мобильные носители, так и сетевые соединения — фактически все каналы, по которым можно скопировать файл. Однако, в отличие от червей, вирусы не используют сетевые ресурсы — заражение вирусом возможно, только если пользователь сам каким-либо образом его активировал, например скопировал или получил по почте зараженный файл и сам его запустил или просто открыл.

После проникновения следует активация вируса. Это может происходить разными путями, и в зависимости от выбранного метода вирусы делятся на такие виды:

- *загрузочные вирусы* заражают загрузочные сектора жестких дисков и мобильных носителей;
- *файловые вирусы* заражают файлы.

Дополнительным признаком отличия вирусов от других вредоносных программ служит их привязанность к операционной системе или программной оболочке, для которой каждый конкретный вирус был написан. Так, вирус для Microsoft Windows не будет работать и заражать файлы на компьютере с другой установленной операционной системой, например UNIX.

При подготовке своих копий вирусы могут применять для маскировки разные технологии:

- *шифрование* — в этом случае вирус состоит из двух частей: сам вирус и шифратор;
- *метаморфизм* — при применении этого метода вирусные копии создаются путем замены некоторых команд на аналогичные, перестановки местами частей кода, вставки между ними дополнительных, обычно ничего не делающих команд.

Соответственно, в зависимости от используемых методов маскировки вирусы можно делить на шифрованные, метаморфные и полиморфные, использующие комбинацию двух типов маскировки.

Сетевые черви

В отличие от вирусов сетевые черви — это вполне самостоятельные вредоносные программы. Главной их особенностью также явля-

ется способность к саморазмножению, однако при этом они способны к самостоятельному распространению с использованием сетевых каналов.

В зависимости от способа проникновения в систему черви делятся на следующие типы:

- *сетевые черви* используют для распространения локальные сети и Интернет;
- *почтовые черви* распространяются с помощью почтовых программ;
- *IM-черви* используют программы обмена сообщениями IM (Instant Messenger) в режиме реального времени;
- *IRC-черви* распространяются через чаты IRC (Internet Relay Chat);
- *P2P-черви* распространяются при помощи пиринговых файлообменных сетей P2P (Peer-to-Peer — равный с равным).

После проникновения на компьютер червь должен активироваться — иными словами, запуститься. По методу активации все черви можно разделить на две большие группы: на тех, которые требуют активного участия пользователя, и тех, кто его не требует.

Отличительная особенность червей из первой группы — это использование обманных методов. Например, получатель инфицированного файла вводится в заблуждение текстом полученного письма и добровольно открывает вложение с почтовым червем, тем самым его активируя. Черви из второй группы используют ошибки в настройке или бреши в системе безопасности операционной системы. В последнее время наметилась тенденция к совмещению этих двух технологий — такие черви наиболее опасны и часто вызывают глобальные эпидемии.

Сетевые черви могут кооперироваться с вирусами — такая пара способна самостоятельно распространяться по сети (благодаря червю) и в то же время заражать ресурсы компьютера (функции вируса).

Троянские программы

Троянская программа (программа класса «троянский конь», или просто троян) имеет только одно назначение — нанести ущерб целевому компьютеру путем выполнения не санкционированных пользователем действий: кражи, порчи или удаления конфиденциальных данных, нарушения работоспособности компьютера или использования его ресурсов в неблаговидных целях.

В отличие от вирусов и червей, трояны сами не размножаются. Жизненный цикл троянов состоит всего из трех этапов:

- проникновение в систему;
- активация;
- выполнение вредоносных действий.

Некоторые трояны способны к самостоятельному преодолению систем защиты компьютерной системы с целью проникновения в нее. В этом случае обычно применяется маскировка, когда троян выдает

себя за полезное приложение, которое пользователь самостоятельно копирует себе на диск (например, загружает из Интернета) и запускает. При этом программа действительно может быть полезна, однако наряду с основными функциями она может выполнять действия, свойственные трояну.

Однако в большинстве случаев трояны проникают на компьютеры вместе с вирусом либо червем — т. е. такие трояны можно рассматривать как дополнительную вредоносную нагрузку, но не как самостоятельную программу.

После проникновения на компьютер трояну необходима активация, и здесь он похож на червя — либо требует активных действий от пользователя, либо через уязвимости в программном обеспечении самостоятельно заражает систему.

Поскольку главная цель троянов — это выполнение несанкционированных действий, они классифицируются по типу вредоносной нагрузки:

- *похитители паролей* предназначены для кражи паролей путем поиска на зараженном компьютере специальных файлов, которые их содержат;
- *утилиты скрытого удаленного управления* — это трояны, которые обеспечивают несанкционированный удаленный контроль над инфицированным компьютером. Обычно это возможность скрыто загружать, отсылать, запускать или уничтожать файлы. Такие трояны могут быть использованы как для получения конфиденциальной информации, так и для запуска вирусов, уничтожения данных;
- *логические бомбы* характеризуются способностью при срабатывании заложенных в них условий (в конкретный день, время суток, в ответ на определенное действие пользователя или команды извне) выполнять какое-либо действие, например удаление файлов;
- *клавиатурные шпионы*, постоянно находясь в оперативной памяти, записывают все данные, поступающие от клавиатуры, с целью последующей их передачи своему автору;
- *анонимные SMTP- и прокси-серверы* — такие трояны на зараженном компьютере организуют несанкционированную отправку электронной почты, что часто используется для рассылки спама;
- *утилиты дозвона* в скрытом от пользователя режиме инициируют подключение к платным сервисам Интернета;
- *модификаторы настроек браузера* меняют стартовую страницу в браузере, страницу поиска или еще какие-либо настройки, открывают дополнительные окна, имитируют нажатия на рекламные баннеры и т. п.

Отдельно отметим, что существуют программы из класса троянов, которые наносят вред другим, удаленным компьютерам и сетям, при этом не нарушая работоспособности инфицированного компьютера. Яркие представители этой группы — *организаторы DDoS-атак.*

Другие вредоносные программы и нежелательная корреспонденция

Кроме вирусов, червей и троянов существует еще много других вредоносных программ и нежелательной корреспонденции. Среди них можно выделить следующие группы:

- *шпионское ПО (Spyware)* — опасные для пользователя программы, предназначенные для слежения за системой и отсылки собранной информации третьей стороне — создателю или заказчику такой программы. Среди заказчиков шпионского ПО — спамеры, рекламщики, маркетинговые агентства, скам-агентства, преступные группировки, деятели промышленного шпионажа. Шпионские программы интересуются системными данными, типом браузера, посещаемыми веб-узлами, иногда и содержимым файлов на жестком диске компьютера-жертвы. Такие программы тайно закачиваются на компьютер вместе с каким-нибудь бесплатным софтом или при просмотре определенным образом сконструированных HTML-страниц и всплывающих рекламных окон и самоустанавливаются без информирования об этом пользователя. Побочные эффекты от присутствия шпионского ПО на компьютере — нестабильная работа браузера и замедление производительности системы;
- *условно опасные программы*, о которых нельзя однозначно сказать, что они вредоносны. Такие программы обычно становятся опасными только при определенных условиях или действиях пользователя. К ним относятся:
  - *апплеты (applets)* — прикладные программы, небольшие Java-приложения, встраиваемые в HTML-страницы. По своей сути эти программы не вредоносные, но могут использоваться в злонамеренных целях. Особенно апплеты опасны для любителей онлайновых игр, так как в них апплеты Java требуются обязательно. Апплеты, как и шпионское ПО, могут использоваться для отправки собранной на компьютере информации третьей стороне;
  - *рекламные утилиты (adware)* — условно-бесплатные программы, которые в качестве платы за свое использование демонстрируют пользователю рекламу, чаще всего в виде графических баннеров. После официальной оплаты и регистрации обычно показ рекламы заканчивается и программы начинают работать в обычном режиме. Проблема рекламных утилит кроется в механизмах, которые используются для загрузки рекламы на компьютер. Кроме того, что для этих целей часто используются программы сторонних и не всегда проверенных производителей, даже после регистрации такие модули могут автоматически не удаляться и продолжать свою работу в скрытом режиме;
  - *riskware* — вполне легальные программы, которые сами по себе не опасны, но обладают функционалом, позволяющим злоумышленнику использовать их с вредоносными целями.

К riskware относятся обычные утилиты удаленного управления, которыми часто пользуются администраторы больших сетей, клиенты IRC, программы для загрузки файлов из Интернета, утилиты восстановления забытых паролей и др.;
— *хакерские утилиты* — к этому виду программ относятся программы сокрытия кода зараженных файлов от антивирусной проверки (шифровальщики файлов), автоматизации создания сетевых червей, компьютерных вирусов и троянских программ (конструкторы вирусов), наборы программ, которые используют хакеры для скрытного взятия под контроль взломанной системы (RootKit), и другие подобные утилиты. Такие специфические программы обычно используют только хакеры;

- *мистификации* — программы, которые намеренно вводят пользователя в заблуждение путем показа уведомлений, например, о форматировании диска или обнаружении вирусов, хотя на самом деле ничего не происходит. Текст таких сообщений зависит от фантазии автора программы;
- *спам* — нежелательная почтовая корреспонденция рекламного характера, загружающая трафик и отнимающая время у пользователей.

14.2. Основы работы антивирусных программ

Самыми эффективными средствами защиты от вирусов являются специальные программы, способные распознавать и обезвреживать вирусы в файлах, письмах и других объектах. Такие программы называются антивирусами, и для того, чтобы построить действительно надежную антивирусную защиту, использовать их нужно обязательно.

В современных антивирусных продуктах используется два основных подхода к обнаружению вредоносных программ: сигнатурный и проактивный/эвристический.

Сигнатурные методы — точные методы обнаружения вирусов, основанные на сравнении файла с известными образцами вирусов.

Проактивные/эвристические методы — приблизительные методы обнаружения, которые позволяют с определенной вероятностью предположить, что файл заражен.

14.2.1. Сигнатурный анализ

Термин «сигнатура» происходит от английского слова signature, означающего «подпись», или же в переносном смысле «характерная черта, нечто идентифицирующее».

Сигнатурный анализ заключается в выявлении характерных идентифицирующих черт каждого вируса и поиска вирусов путем сравнения файлов с выявленными чертами [84].

Сигнатурой вируса будет считаться совокупность черт, позволяющих однозначно идентифицировать наличие вируса в файле (включая случаи, когда файл целиком является вирусом). Все вместе сигнатуры известных вирусов составляют *антивирусную базу*.

Эта технология предполагает непрерывное отслеживание новых экземпляров вредителей, их описание и включение в базу сигнатур. Задачу выделения сигнатур, как правило, решают люди — эксперты в области компьютерной вирусологии, способные выделить код вируса из кода программы и сформулировать его характерные черты в форме, наиболее удобной для поиска. В наиболее простых случаях могут применяться специальные автоматизированные средства выделения сигнатур, например для несложных по структуре троянов или червей, которые не заражают другие программы, а целиком являются вредоносными программами.

Практически в каждой компании, выпускающей антивирусы, есть своя группа экспертов, выполняющая анализ новых вирусов и пополняющая антивирусную базу новыми сигнатурами. По этой причине антивирусные базы в разных антивирусах отличаются. Тем не менее между антивирусными компаниями существует договоренность об обмене образцами вирусов, а значит, рано или поздно сигнатура нового вируса попадает в антивирусные базы практически всех антивирусов. Лучшим же антивирусом будет тот, для которого сигнатура нового вируса была выпущена раньше всех.

Часто для обнаружения семейства похожих вирусов используется одна сигнатура, и поэтому количество сигнатур не всегда равно количеству обнаруживаемых вирусов. Соотношение количества сигнатур и числа известных вирусов для каждой антивирусной базы свое. Если же учесть, что антивирусные компании обмениваются образцами вирусов, можно с высокой долей уверенности считать, что антивирусные базы наиболее известных антивирусов эквивалентны.

Важное дополнительное свойство сигнатур — точное и гарантированное определение типа вируса. Это свойство позволяет занести в базу не только сами сигнатуры, но и способы лечения вируса.

Главные критерии эффективности сигнатурного метода — это скорость реакции на новые угрозы, частота обновлений, максимальное число обнаруженных угроз.

Главный недостаток сигнатурного метода — задержка при реакции на новые угрозы. Для получения сигнатуры необходимо иметь образец вируса. Создать его сигнатуру невозможно, пока вирус не попал на анализ к экспертам. Поэтому сигнатуры всегда появляются только через некоторое время после появления нового вируса. Именно поэтому сигнатурный метод непригоден для оперативной защиты от вновь появляющихся вирусов.

С момента появления вируса в сети Интернет до выпуска первых сигнатур обычно проходит несколько часов, и все это время вирус способен заражать компьютеры почти беспрепятственно. Почти — потому что в защите от новых вирусов помогают используемые в антивирусных программах проактивные/эвристические методы обнаружения вирусов.

14.2.2. Проактивные методы обнаружения

Проактивные методы обнаружения вирусов получают все большее распространение. В принципе, использование этой технологии позволяет обнаруживать еще неизвестные вредоносные программы. Существует несколько подходов к проактивной защите.

Рассмотрим два наиболее популярных подхода: эвристические анализаторы и поведенческие блокираторы [84].

Эвристические анализаторы

Слово «эвристика» происходит от греческого глагола «находить». Суть *эвристических методов* состоит в том, что решение проблемы основывается на некоторых правдоподобных предположениях, а не на строгих выводах из имеющихся фактов и предпосылок. Такое определение звучит достаточно сложно, поэтому эвристический метод поясним далее на примерах.

Если сигнатурный метод основан на выделении характерных признаков вируса и поиске этих признаков в проверяемых файлах, то эвристический анализ основывается на предположении (весьма правдоподобном), что новые вирусы часто оказываются похожи на какие-либо из уже известных. Такое предположение оправдывается наличием в антивирусных базах сигнатур для определения не одного, а сразу нескольких вирусов. Этот эвристический метод часто называют *поиском вирусов, похожих на известные*, или *статическим анализом*.

Эвристический анализатор (эвристик) — это программа, которая анализирует программный код проверяемого объекта и по косвенным признакам определяет, является ли объект вредоносным. Работа эвристического анализатора, как правило, начинается с поиска в программном коде подозрительных признаков (команд), характерных для вредоносных программ.

Например, многие вредоносные коды ищут исполняемые программы, открывают найденные файлы и изменяют их. Эвристический анализатор просматривает код приложения и, встретив подозрительную команду, увеличивает некий «счетчик подозрительности» для данного приложения. Если после просмотра всего кода значение счетчика превышает заданное пороговое значение, то объект признается подозрительным.

Первые эвристические анализаторы появились в антивирусных продуктах довольно давно, и на сегодняшний день более или менее совершенные эвристики реализованы во всех антивирусных решениях.

Достоинствами статического анализа являются простота реализации, высокая скорость работы, возможность обнаружения новых неизвестных вирусов еще до того, как для них будут выделены сигнатуры.

Однако уровень обнаружения новых вредоносных кодов остается довольно низким, а вероятность ложных срабатываний высокой. По-

этому в современных антивирусах статический анализ используется в сочетании с динамическим.

Идея такого комбинированного подхода состоит в том, чтобы до того, как приложение будет запущено на компьютере пользователя, эмулировать его запуск в безопасном виртуальном окружении, которое называется также буфером эмуляции, или «песочницей».

Динамический эвристический анализатор читает часть кода приложения в буфер эмуляции антивируса и с помощью специальных приемов эмулирует его исполнение. Если в процессе этого псевдоисполнения обнаруживаются какие-либо подозрительные действия, объект признается вредоносным и его запуск на компьютере пользователя блокируется.

В отличие от статического метода, динамический более требователен к ресурсам ПК, так как для анализа приходится использовать безопасное виртуальное пространство, а запуск приложения на компьютере пользователя откладывается на время анализа. Однако и уровень обнаружения вредителей у динамического метода значительно выше статического, а вероятность ложных срабатываний существенно меньше.

Недостатки эвристических анализаторов:

- невозможность лечения — в силу потенциальных ложных срабатываний и возможного неточного определения типа вируса попытка лечения может привести к бо́льшимпотерям информации, чем из-за самого вируса, а это недопустимо;
- низкая эффективность против принципиально новых типов вирусов.

Поведенческие блокираторы

Поведенческий блокиратор — это программа, которая анализирует поведение запущенного приложения и блокирует любые опасные действия.

К основным вредоносным действиям относят:

- удаление файла;
- запись в файл;
- запись в определенные области системного реестра;
- открытие порта на прослушивание;
- перехват данных, вводимых с клавиатуры;
- рассылка писем и др.

Выполнение каждого такого действия по отдельности не дает повода считать программу вредоносной. Но если программа последовательно выполняет несколько таких действий, например перехватывает данные, вводимые с клавиатуры, и с определенной частотой пересылает их на какой-то адрес в Интернете, значит, эта программа по меньшей мере подозрительна.

В отличие от эвристических анализаторов, где подозрительные действия отслеживаются в режиме эмуляции (динамический эвристик), поведенческие блокираторы работают в реальных условиях.

Принцип действия первых поведенческих блокираторов был прост. При обнаружении потенциально опасного действия задавался вопрос пользователю: разрешить или запретить это действие. Во многих случаях такой подход работал, но «подозрительные» действия производили и легитимные программы (вплоть до операционной системы). Поэтому, если пользователь не обладал должной квалификацией, вопросы антивируса вызывали непонимание.

Современные поведенческие блокираторы анализируют уже не отдельные действия, а последовательность операций. Другими словами, заключение об опасности того или иного приложения выносится на основе более сложного анализа. Таким образом, удается значительно сократить количество запросов к пользователю и повысить надежность детектирования.

Современные поведенческие блокираторы способны контролировать широкий спектр событий, происходящих в системе. Это прежде всего контроль опасной активности (анализ поведения всех процессов, запущенных в системе, сохранение всех изменений, производимых в файловой системе и реестре).

При выполнении некоторым приложением набора подозрительных действий выдается предупреждение пользователю об опасности данного процесса. Помимо этого блокиратор позволяет перехватить все возможности внедрения программного кода в чужие процессы. Вдобавок блокиратор способен обнаружить *руткиты*, т. е. программы, которые скрывают от пользователя работу вредоносного кода с файлами, папками и ключами реестра, а также прячут запущенные программы, системные службы, драйверы и сетевые соединения.

Особо стоит выделить такую функциональность поведенческих блокираторов, как контроль целостности приложений и системного реестра Microsoft Windows. В последнем случае блокиратор контролирует изменения ключей реестра и позволяет задавать правила доступа к ним для различных приложений. Все вместе это позволяет осуществить откат изменений после определения опасной активности в системе. Таким образом, можно восстанавливать систему даже после вредоносных действий неизвестных программ, вернув ее к незараженному состоянию.

В качестве примера эффективного поведенческого блокиратора нового поколения можно привести модуль проактивной защиты (Proactive Defence Module), реализованный в продуктах Лаборатории Касперского. Данный модуль включает в себя все перечисленные выше возможности и, что особенно важно, хорошую систему информирования пользователя о том, в чем реально состоит опасность тех или иных подозрительных действий. Любой поведенческий блокиратор на определенном этапе требует вмешательства пользователя, что предполагает наличие у последнего определенной квалификации. На практике пользователь часто не обладает необходимыми знаниями, поэтому информационная поддержка — фактически поддержка принятия решений — является обязательным атрибутом современных антивирусных решений.

Поведенческий блокиратор может предотвратить распространение как известного, так и неизвестного (написанного после создания блокиратора) вируса, что является неоспоримым достоинством такого подхода к защите.

Недостатком поведенческих блокираторов остается срабатывание на действия ряда легитимных программ. Для принятия окончательного решения о вредоносности приложения требуется вмешательство пользователя, что предполагает наличие у него достаточной квалификации.

Проактивный подход к борьбе с вредоносными программами стал ответом разработчиков антивирусов на все возрастающий поток новых вредителей и увеличивающуюся скорость их распространения. Существующие сегодня проактивные методы действительно позволяют бороться со многими новыми угрозами. Однако проактивные технологии не позволяют полностью отказаться от обновлений антивирусной защиты. Проактивные методы так же, как и сигнатурные, требуют регулярных обновлений.

Для оптимальной антивирусной защиты необходимо сочетание проактивных и сигнатурных подходов. Максимального уровня обнаружения угроз можно достигнуть, только комбинируя эти методы. Примером успешного сочетания проактивных и сигнатурных методов может служить технология ThreatSense компании Eset.

ThreatSense — это сбалансированная технология, позволяющая комбинировать эвристический анализатор и поведенческий блокиратор с сигнатурным методом. Эта технология обеспечивает обнаружение не только известных, но и новых угроз, не снижая при этом скорости работы используемой системы.

Практически любая антивирусная программа объединяет в разных пропорциях все технологии и методы защиты от вирусов, созданные к сегодняшнему дню.

14.2.3. Дополнительные модули

Практически любой антивирус сегодня использует все известные методы обнаружения вирусов. Но одних средств обнаружения мало для успешной работы антивируса — для того чтобы чисто антивирусные средства были эффективными, нужны дополнительные модули, выполняющие вспомогательные функции.

Модуль обновления

Каждый антивирус должен содержать модуль обновления. Это связано с тем, что основным методом обнаружения вирусов сегодня является сигнатурный анализ, который полагается на использование антивирусной базы.

Чтобы сигнатурный анализ эффективно справлялся с самыми последними вирусами, антивирусные эксперты постоянно анализируют

образцы новых вирусов и выпускают для них сигнатуры. После этого главной проблемой становится доставка сигнатур на компьютеры всех пользователей, использующих соответствующую антивирусную программу. Именно эту задачу и решает модуль обновления.

После того как эксперты создали новые сигнатуры, файлы с сигнатурами размещаются на серверах компании-производителя антивируса и становятся доступными для загрузки. Модуль обновления обращается к этим серверам, определяет наличие новых файлов, загружает их на компьютер пользователя и дает команду антивирусным модулям использовать новые файлы сигнатур.

Модуль планирования

Модуль планирования является вторым важным вспомогательным модулем. Существует ряд действий, которые антивирус должен выполнять регулярно: проверять весь компьютер на наличие вирусов и обновлять антивирусную базу.

В настоящее время новые модификации вредоносных программ обнаруживаются постоянно, что вынуждает антивирусные компании выпускать новые файлы сигнатур для обновления антивирусной базы буквально каждый час. Разумным расписанием для компьютера можно считать проверку раз в неделю. Модуль планирования позволяет настроить периодичность выполнения этих действий.

Модуль управления

По мере увеличения количества модулей в антивирусе возникает необходимость в дополнительном модуле для управления и настройки. Основные требования к такому модулю — удобный доступ к настройкам, интуитивная понятность, подробная справочная система, описывающая каждую настройку, возможность защитить настройки от изменений, если за компьютером работает несколько человек. Подобным модулем управления обладают антивирусы для домашнего использования.

Антивирусы для защиты компьютеров в крупных сетях должны обладать несколько иными свойствами. Такие антивирусы оборудованы специальным модулем управления.

Основные свойства этого модуля управления:

- *поддержка удаленного управления и настройки* — администратор безопасности может запускать и останавливать антивирусные модули, а также менять их настройки по сети, не вставая со своего места;
- *защита настроек от изменений* — модуль управления не позволяет локальному пользователю изменять настройки или останавливать антивирус, чтобы пользователь не мог ослабить антивирусную защиту организации.

Карантин

Во многих антивирусах среди вспомогательных средств имеется специальная технология — карантин, — которая защищает от возможной потери данных в результате действий антивируса.

Например, нетрудно представить ситуацию, при которой файл детектируется как возможно зараженный эвристическим анализатором и удаляется согласно настройкам антивируса.

Однако эвристический анализатор никогда не дает стопроцентной гарантии того, что файл действительно заражен, а значит, с определенной вероятностью антивирус мог удалить незараженный файл. Или же антивирус обнаруживает важный документ, зараженный вирусом, и пытается согласно настройкам выполнить лечение, но по каким-то причинам происходит сбой и вместе с вылеченным вирусом теряется важная информация.

От таких случаев желательно застраховаться. Это можно сделать, если перед лечением или удалением файлов сохранить их резервные копии, тогда, если окажется, что файл был удален ошибочно или потеряна важная информация, всегда можно будет выполнить восстановление из резервной копии.

14.2.4. Режимы работы антивирусов

Надежность антивирусной защиты обеспечивается не только способностью отражать любые вирусные атаки. Другое не менее важное свойство защиты — ее непрерывность. Это означает, что антивирус должен начинать работу по возможности до того, как вирусы смогут заразить только что включенный компьютер, и выключаться только после завершения работы всех программ.

Однако, с другой стороны, пользователь должен иметь возможность в любой момент запросить максимум ресурсов компьютера для решения своей прикладной задачи и антивирусная защита не должна ему мешать это сделать. Оптимальный выход в этой ситуации — это введение двух различных режимов работы антивирусных средств:

- непрерывная проверка на наличие вирусов с небольшой функциональностью в режиме реального времени;
- тщательная проверка на наличие вирусов по запросу пользователя.

Проверка в режиме реального времени

Проверка в режиме реального времени обеспечивает непрерывность работы антивирусной защиты. Это реализуется с помощью обязательной проверки всех действий, совершаемых другими программами и самим пользователем, на предмет вредоносности вне зависимости от их исходного расположения — будь то свой жесткий диск,

внешние носители информации, другие сетевые ресурсы или собственная оперативная память. Также проверке подвергаются все косвенные действия через третьи программы. Режим постоянной проверки защиты системы от заражения должен быть включен с момента начала загрузки операционной системы и выключаться только в последнюю очередь.

Проверка по требованию

В некоторых случаях наличия постоянно работающей проверки в режиме реального времени может быть недостаточно. Допустим, что на компьютер был скопирован зараженный файл, исключенный из постоянной проверки ввиду больших размеров, и следовательно, вирус в нем обнаружен не был. Если этот файл на рассматриваемом компьютере запускаться не будет, то вирус может проявить себя только после пересылки его на другой компьютер, что может сильно повредить репутации отправителя — распространителя вирусов. Для исключения подобных случаев используется второй режим работы антивируса — проверка по требованию.

Для такого режима пользователь обычно сам указывает, какие файлы, каталоги или области диска необходимо проверить, и время, когда нужно произвести такую проверку, — в виде расписания или разового запуска вручную. Рекомендуется проверять все чужие внешние носители информации, такие как дискеты, компакт-диски, флэш-накопители, каждый раз перед чтением информации с них, а также весь свой жесткий диск не реже одного раза в неделю.

Тестирование работы антивируса

После того как антивирус установлен и настроен, необходимо убедиться, что все сделано правильно и антивирусная защита работает. Как проверить работу антивируса?

Использовать для тестирования настоящие вирусы крайне опасно. Если пользователь неправильно выполнил установку или настройку антивируса, то в процессе такого тестирования он может заразить свой компьютер, потеряв в результате данные или став источником заражения для других компьютеров.

Нужен такой способ тестирования антивирусов, который был бы безопасным, но давал четкий ответ на вопрос, корректно ли работает антивирус.

Учитывая важность проблемы, организация EICAR при участии антивирусных компаний создала специальный тестовый файл, названный по имени организации — eicar.com.

Eicar.com — это исполняемый файл в COM-формате, который не выполняет никаких вредоносных действий, а просто выводит на экран строку «EICAR-STANDARD-ANTIVIRUS-TEST-FILE!».

Получить eicar.com можно на сайте организации EICAR по адресу *http://www.eicar.org/anti_virus_test_file.htm*, но можно создать этот файл самостоятельно, используя редактор Notepad системы Windows.

Файл eicar.com позволяет протестировать, как антивирус справляется с файловыми вирусами и близкими по структуре вредоносными программами — большинством троянов, некоторыми червями.

14.2.5. Антивирусные комплексы

Второй способ оптимизации работы антивируса — это создание различных его версий для компьютеров, служащих разным целям. Зачастую они отличаются лишь наличием тех или иных специфических модулей и различием в интерфейсе, в то время как непосредственно антивирусная проверка осуществляется одной и той же подпрограммой, называемой антивирусным ядром.

Антивирусный комплекс — набор антивирусов, использующих одинаковое антивирусное ядро, предназначенный для решения практических проблем по обеспечению антивирусной безопасности компьютерных систем. В антивирусный комплекс также в обязательном порядке входят средства обновления антивирусных баз.

Всякая локальная сеть, как правило, содержит компьютеры двух типов: рабочие станции, за которыми непосредственно сидят люди, и сетевые серверы, используемые для служебных целей. В соответствии с характером выполняемых функций серверы делятся на:

- *сетевые*, которые обеспечивают централизованное хранилище информации: файловые серверы, серверы приложений и др.;
- *почтовые*, на которых работает программа, служащая для передачи электронных сообщений от одного компьютера к другому;
- *шлюзы*, отвечающие за передачу информации из одной сети в другую. Например, шлюз необходим для соединения локальной сети с Интернетом.

Соответственно, различают четыре вида антивирусных комплексов — для защиты рабочих станций, файловых серверов, почтовых систем и шлюзов.

Рабочие станции — это компьютеры локальной сети, за которыми непосредственно работают пользователи. Главной задачей комплекса для защиты рабочих станций является обеспечение безопасной работы на рассматриваемом компьютере — для этого необходима проверка в режиме реального времени, проверка по требованию и проверка локальной электронной почты.

Сетевые серверы — это компьютеры, специально выделенные для хранения или обработки информации. Они обычно не используются для непосредственной работы за ними, и поэтому, в отличие от рабочих станций, проверка электронной почты на наличие вирусов тут не нужна. Следовательно, антивирусный комплекс для файловых серверов

должен производить проверку в режиме реального времени и проверку по требованию.

Антивирусный комплекс для защиты *почтовых систем* предназначен для проверки всех проходящих электронных писем на наличие в них вирусов. То есть проверять другие файлы, размещенные на этом компьютере, он не обязан (для этого существует комплекс защиты сетевых серверов). Поэтому к нему предъявляются требования по наличию собственно программы для проверки всей принимаемой и отправляемой почтовой корреспонденции в режиме реального времени и дополнительно механизма проверки по требованию почтовых баз данных.

Аналогично, в соответствии со своим назначением, антивирусный комплекс для *шлюза* осуществляет только проверку проходящих через шлюз данных.

Поскольку все вышеперечисленные комплексы используют сигнатурный анализ, то в обязательном порядке в них должно входить средство для поддержания антивирусных баз в актуальном состоянии, т. е. механизм их обновления. Дополнительно часто оказывается полезным модуль для удаленного централизованного управления, который позволяет системному администратору со своего рабочего места настраивать параметры работы антивируса, запускать проверку по требованию и обновление антивирусных баз.

14.2.6. Дополнительные средства защиты

Возможности антивирусных программ расширяют дополнительные средства защиты от вредоносных программ и нежелательной корреспонденции.

Такими средствами защиты являются:

- обновления, устраняющие уязвимости в операционной системе, через которые могут проникать вирусы;
- брандмауэры — программы, защищающие от атак по сети;
- средства борьбы со спамом.

Обновления ПО

Как известно, вирусы нередко проникают на компьютеры через уязвимости в операционной системе или установленных программах. Причем чаще всего вредоносными программами используются уязвимости операционной системы Microsoft Windows, пакета приложений Microsoft Office, браузера Internet Explorer и почтовой программы Outlook Express.

Чтобы не дать вирусам возможности использовать уязвимость, операционную систему и программное обеспечение нужно обновлять. Производители, как правило, раньше вирусописателей узнают о ды-

рах в своих программах и заблаговременно выпускают для них исправления.

Для загрузки и установки обновлений в большинстве программ и систем есть встроенные средства. Например, в Windows XP и Windows Vista имеется специальный компонент **Автоматическое обновление**, параметры работы которого настраиваются в окне **Свойства системы**.

В последнее время вредоносные программы, использующие уязвимости в Windows и прикладных программах, появляются вскоре после выхода исправлений к этим уязвимостям. В некоторых случаях вредоносные программы появляются даже раньше исправлений. Поэтому необходимо своевременно устанавливать исправления, используя для этого средства автоматической установки.

Брандмауэры

Для того чтобы удаленно воспользоваться уязвимостью в программном обеспечении или операционной системе, нужно установить соединение и передать специально сформированный пакет данных. От таких попыток проникновения и заражения можно защититься путем запрета определенных соединений. Задачу контроля соединений успешно решают программы-брандмауэры.

Брандмауэр — это программа, которая следит за сетевыми соединениями и принимает решение о разрешении или запрещении новых соединений на основании заданного набора правил.

Правило брандмауэра задается несколькими атрибутами:

- *приложение* — определяет программу, к которой относится правило, так что одни и те же действия могут быть разрешены одним программам и запрещены другим. Например, получать и отправлять почту разумно разрешить только почтовому клиенту;
- *протокол* — определяет протокол, используемый для передачи данных. Обычно можно выбрать между двумя протоколами — TCP и UDP;
- *адреса* — определяет, для соединений с каких адресов или на какие адреса будет действовать правило;
- *порт* — задает номера портов, на которые распространяется правило;
- *направление* — позволяет отдельно контролировать входящие и исходящие соединения;
- *действие* — определяет реакцию на обнаружение соединения, соответствующего остальным параметрам. Реакция может быть следующей: разрешить, запретить или спросить у пользователя.

Необязательно задавать конкретные значения всем атрибутам правила. Можно создать правило, которое будет запрещать входящие соединения на TCP-порт 111 для всех приложений или разрешать любые исходящие соединения для программы Internet Explorer.

Для борьбы с вирусами брандмауэры могут применяться следующим образом.

Во-первых, брандмауэр можно успешно использовать для защиты от вредоносных программ, которые распространяются непосредственно по сети, используя уязвимости в операционной системе. Например, червь Sasser атакует службу Windows LSASS через TCP-порт 445. Для защиты от червя достаточно создать в брандмауэре правило, запрещающее входящие соединения на этот порт. Брандмауэр можно использовать и для защиты от атак неизвестных вирусов.

Второй способ применения брандмауэров для защиты от вредоносных программ состоит в контроле исходящих соединений. Многие троянские программы, да и черви, после выполнения вредоносной функции стремятся подать сигнал автору вируса. Например, троянская программа, ворующая пароли, будет пытаться переслать все найденные пароли на определенный сайт или почтовый адрес. Для того чтобы воспрепятствовать этому, можно настроить брандмауэр на блокирование всех неизвестных соединений: разрешить только соединения от доверенных программ, таких как используемый браузер, почтовый клиент, программа мгновенного обмена сообщений, а все остальные соединения запретить.

Некоторые вредоносные программы пассивно ожидают соединения на каком-то из портов. Если входящие соединения разрешены, то автор вредоносной программы сможет через некоторое время обратиться на этот порт и забрать нужную ему информацию или же передать вредоносной программе новые команды. Чтобы этого не произошло, брандмауэр должен быть настроен на запрет входящих соединений на все порты, кроме фиксированного перечня портов, используемых известными программами или операционной системой.

В последнее время широко распространены универсальные защитные программы, объединяющие возможности брандмауэра и антивируса, например Kaspersky Internet Security, Norton Internet Security, McAfee Internet Security и пр.

Средства защиты от нежелательной корреспонденции

Для решения проблемы защиты от спама (нежелательной корреспонденции рекламного характера) используются специальные антиспамовые фильтры. Для фильтрации нежелательной почты в антиспамовых фильтрах применяется несколько методов:

- *черные и белые списки адресов.* Черный список — это список тех адресов, письма с которых фильтр отбраковывает сразу, не применяя других методов. В этот список нужно заносить адреса, если с них постоянно приходят ненужные или, хуже того, зараженные письма. Белый список — это список адресов хорошо известных пользователю людей или организаций, которые передают только полезную информацию. Антиспамовый фильтр можно настроить

так, что будут приниматься только письма от адресатов из белого списка;

- *базы данных образцов спама.* Как и антивирус, антиспамовый фильтр может использовать базу данных образцов нежелательных писем для удаления писем, соответствующих этим образцам;
- *анализ служебных заголовков.* В письме в относительно скрытой форме хранится служебная информация о том, с какого сервера было доставлено письмо, какой адресат является реальным отправителем и др. Используя эту информацию, антиспамовый фильтр может решать, является письмо спамом или нет. Например, некоторые почтовые серверы, часто используемые для рассылки спама, заносятся в специальные общедоступные черные списки, и если письмо было доставлено с такого сервера, вполне вероятно, что это спам. Другой вариант проверки — запросить у почтового сервера, действительно ли существует адресат, указанный в письме как отправитель. Если такого адресата не существует, значит, письмо, скорее всего, является нежелательным;
- *самообучение.* Антиспамовые фильтры можно обучать, указывая вручную, какие письма являются нормальными, а какие нежелательными. Через некоторое время антиспамовый фильтр начинает с большой достоверностью самостоятельно определять нежелательные письма по их похожести на предыдущий спам и непохожести на предыдущие нормальные письма.

Использование антиспамовых фильтров помогает защититься и от некоторых почтовых червей. Самое очевидное применение — это при получении первого зараженного письма (в отсутствие антивируса это можно определить по косвенным признакам) отметить его как нежелательное — и в дальнейшем все другие зараженные письма будут заблокированы фильтром.

Более того, почтовые черви известны тем, что имеют большое количество модификаций, незначительно отличающихся друг от друга. Поэтому антиспамовый фильтр может помочь и в борьбе с новыми модификациями известных вирусов с самого начала эпидемии. В этом смысле антиспамовый фильтр даже эффективнее антивируса, так как необходимо дождаться обновления антивирусных баз, чтобы антивирус смог обнаружить новую модификацию.

14.3. Защита корпоративной сети от воздействия вредоносных программ и вирусов

В настоящее время одним из основных вопросов обеспечения безопасности корпоративной информации является защита от вредоносных программ. Защита от вредоносных программ не ограничивается лишь

традиционной установкой антивирусных средств на рабочие станции пользователей. Это сложная задача, требующая комплексного подхода к решению [81, 94].

14.3.1. Подсистема защиты корпоративной информации от вредоносных программ и вирусов

Одно из главных преимуществ данного решения — рассмотрение подсистемы защиты корпоративной информации от вредоносных программ и вирусов как многоуровневой системы (рис. 14.1) [94].

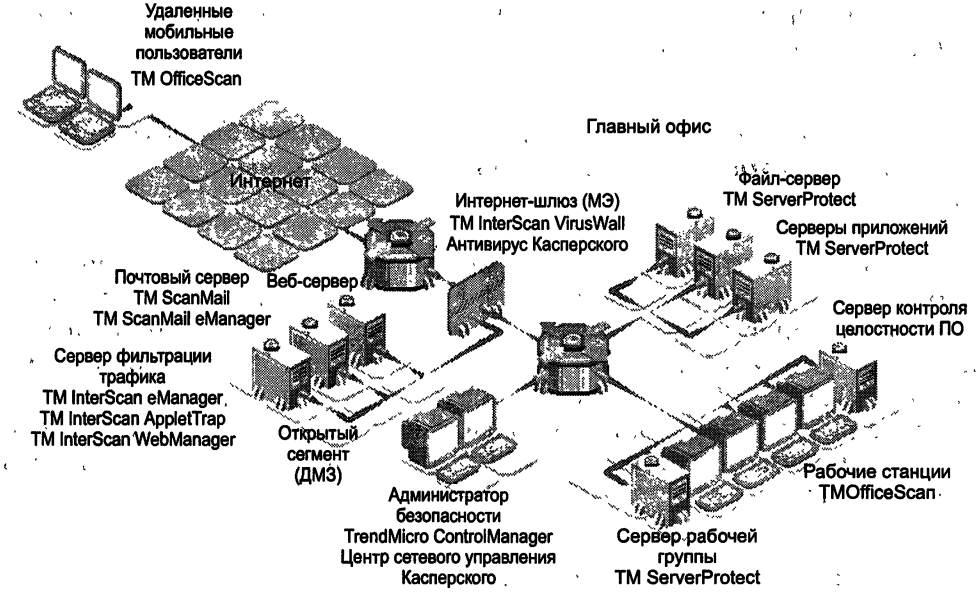


Рис. 14.1. Схема защиты корпоративной сети от воздействия вредоносных программ и вирусов

Первый уровень включает в себя средства защиты от вредоносных программ, устанавливаемые на стыке с глобальными сетями (интернет-шлюз и/или межсетевой экран, публичные серверы (веб-, SMTP-, FTP-), размещаемые в ДМЗ) и осуществляющие фильтрацию основных видов трафика (HTTP, SMTP, FTP и т. д.). Антивирусные средства, устанавливаемые на МЭ, совместимы с Check Point FireWall-1 и Cisco PIX, которые входят в число самых распространенных межсетевых экранов в России.

Второй уровень — средства защиты, устанавливаемые на внутренних корпоративных серверах и серверах рабочих групп (файловых хранилищах, серверах приложений и т. д.).

И наконец, третий уровень — средства защиты от вредоносных программ, устанавливаемые на рабочих станциях пользователей, в том числе удаленных и мобильных.

В качестве средств защиты всех уровней выбраны продукты компании Trend Micro, а на шлюзе в дополнение к продуктам Trend Micro устанавливается антивирус Касперского, повышая тем самым вероятность обнаружения вредоносных программ в точке их наиболее вероятного появления.

Преимущества данного решения заключаются:

- в использовании продуктов мировых лидеров;
- в централизованном управлении всей подсистемой защиты от вредоносных программ;
- в автоматическом обновлении антивирусных баз;
- в тесном взаимодействии антивирусных средств всех уровней подсистемы и т. д.

Все эти преимущества обеспечивают высокую вероятность обнаружения вредоносных программ.

14.3.2. Серия продуктов «Kaspersky Open Space Security» для защиты корпоративных сетей от современных интернет-угроз

Серия продуктов Kaspersky Open Space Security, разработанная в Лаборатории Касперского, включает решения для защиты малых и крупных корпоративных сетей от всех видов современных интернет-угроз [93]. В серии продуктов Kaspersky Open Space Security реализована концепция защиты корпоративной сети, при которой безопасное рабочее пространство больше не ограничено стенами офиса, теперь оно охватывает и удаленных пользователей и сотрудников в командировке.

Основные возможности серии продуктов Kaspersky Open Space Security

Kaspersky Open Space Security полностью отвечает современным требованиям к системам защиты корпоративных сетей:

- решения для защиты каждого узла сети;
- технологии защиты от всех типов интернет-угроз;
- поддержка всех распространенных ОС/платформ;
- высокая скорость реакции на новые угрозы;
- комплексное применение различных технологий защиты.

Kaspersky Open Space Security позволяет в полной мере использовать преимущества новых мобильных технологий, обеспечивая:

- полноценную защиту пользователей за пределами сети;
- комплексную безопасность пользователей смартфонов;
- проверку по возвращении в сеть/проверку «гостей».

Kaspersky Open Space Security использует уникальные технологии для распознавания самых последних уловок злоумышленников:

- защита от утечек информации;

- защита от руткитов;
- отмена вредоносных изменений;
- самозащита антивируса;
- защита данных при потере смартфона.

Kaspersky Open Space Security обеспечивает высокий уровень защиты сложных, распределенных сетей, не теряя удобства и управляемости:

- централизованное администрирование;
- удаленная установка, управление и лечение;
- поддержка самых современных технологий Microsoft, Intel, Cisco;
- эффективное использование сетевых ресурсов.

В серию Kaspersky Open Space Security входит четыре продукта:

- *Kaspersky Work Space Security* — защита рабочих станций (одноуровневая защита). Это решение для централизованной защиты рабочих станций, в том числе ноутбуков, и смартфонов в корпоративной сети и за ее пределами от всех видов современных интернет-угроз: вирусов, шпионских программ, хакерских атак и спама;
- *Kaspersky Business Space Security* — защита рабочих станций и файловых серверов (двухуровневая защита). Это эффективная защита информационных ресурсов компании от современных интернет-угроз. Продукт Kaspersky Business Space Security защищает рабочие станции, смартфоны и файловые серверы от всех видов вирусов, троянских программ и червей, предотвращает вирусные эпидемии, а также обеспечивает сохранность информации и мгновенный доступ пользователей к сетевым ресурсам. Продукт разработан с учетом повышенных требований к серверам, работающим в условиях высоких нагрузок;
- *Kaspersky Enterprise Space Security* — защита рабочих станций, смартфонов, файловых и почтовых серверов (трехуровневая защита). Это решение обеспечивает свободный обмен информацией внутри компании и безопасные коммуникации с внешним миром. Продукт Kaspersky Enterprise Space Security защищает рабочие станции, смартфоны, а также файловые и почтовые серверы от всех видов современных интернет-угроз, удаляет вирусы из потока электронной почты, обеспечивает сохранность информации и мгновенный безопасный доступ пользователей к сетевым ресурсам;
- *Kaspersky Total Space Security* — защита рабочих станций, файловых и почтовых серверов, интернет-шлюзов (многоуровневая защита). Это решение защищает все узлы корпоративной сети любого масштаба и сложности от современных интернет-угроз. Решение Kaspersky Total Space Security контролирует все входящие и исходящие потоки данных — электронную почту, интернет-трафик и все сетевые взаимодействия. Продукт обеспечивает мгновенный и безопасный доступ пользователей к информационным ресурсам компании и сети Интернет, а также гарантирует безопасные коммуникации по электронной почте.

Вопросы для самоконтроля

1. Что такое вредоносная программа? Охарактеризуйте основные типы вредоносных программ.
2. Укажите существенные отличия компьютерных вирусов от сетевых червей. Опишите основные особенности троянских программ.
3. Опишите два основных подхода к обнаружению вредоносных программ.
4. Как выполняется сигнатурный анализ? Каковы его достоинства и недостатки?
5. Что представляют собой проактивные методы обнаружения? Дайте характеристики двух наиболее популярных подходов.
6. Опишите принцип действия, достоинства и недостатки эвристических анализаторов.
7. Опишите принцип действия, достоинства и недостатки поведенческих блокираторов.
8. Назовите и опишите дополнительные модули антивирусных средств.
9. Каковы дополнительные меры и средства защиты от вредоносных программ, расширяющие возможности антивирусных программ?
10. Опишите меры и средства защиты от спама.
11. Каковы особенности реализации подсистемы защиты корпоративной информации от вредоносных программ и вирусов?
12. Каковы возможности серии продуктов Kaspersky Open Space Security для защиты корпоративных сетей от современных интернет-угроз?

ЧАСТЬ IV

УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

Для успешного использования современных информационных технологий необходимо надежное и эффективное управление средствами обеспечения информационной безопасности. И если раньше задача заключалась в управлении отдельными серверами, сетями и маршрутизаторами, то сейчас требуется обеспечить информационную безопасность больших корпоративных систем. Все это предъявляет жесткие требования к управлению средствами информационной безопасности.

Другим важным аспектом управления информационной безопасностью является строгое соблюдение технических и организационно-правовых требований, предъявляемых к системам защиты информации. Эти требования сформулированы в ряде отечественных и международных стандартов по информационной безопасности, а также в руководящих документах (РД) по технической защите информации Государственной технической комиссии (ГТК) России.

Глава 15
УПРАВЛЕНИЕ СРЕДСТВАМИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Корпоративная информационная система — это активный инструмент ведения бизнеса. Эффективная деятельность современного предприятия невозможна без единой корпоративной информационной системы, объединяющей различные бизнес-процессы предприятия. Динамичное развитие бизнеса обусловливает быстрый рост и усложнение корпоративных информационных систем, расширяются их функции и набор предоставляемых сервисов.

Ввиду растущей сложности современного бизнеса компаниям приходится постоянно внедрять все новые и новые технологии, устанавливая более мощное и качественное оборудование. При этом необходимо обеспечить информационную безопасность корпоративных бизнес-процессов, а также надежное и эффективное управление средствами информационной безопасности.

15.1. Задачи управления информационной безопасностью

Важнейшим компонентом корпоративной системы является система управления средствами информационной безопасности предприятия. Сформулируем основные задачи системы управления средствами информационной безопасности предприятия.

Функционально такая система должна решать следующие основные задачи:

- централизованное управление всеми программными и техническими средствами защиты информации;
- управление политикой безопасности в рамках корпоративной информационной системы (КИС) предприятия, формирование локальных политик безопасности (ЛПБ) отдельных устройств и доведения ЛПБ до всех устройств защиты информации;
- распространение обновлений программного обеспечения, а также дополнительных программных средств на рабочие станции и серверы;

- управление конфигурациями объектов и субъектов доступа;
- управление правами доступа к активным сетевым устройствам, рабочим станциям и серверам;
- предоставление сервисов защиты распределенным прикладным системам, регистрация защищенных приложений и их ресурсов;
- управление криптосредствами, в частности криптоключами (ключевая инфраструктура);
- событийное протоколирование; включает настройку выдачи логов на разные устройства, управление уровнем детализации логов, управление составом событий, по которым ведется протоколирование;
- аудит безопасности информационной системы; обеспечивает получение и оценку объективных данных о текущем состоянии защищенности информационной системы; иногда под аудитом безопасности понимают анализ логов, поиск нарушителей и дыр в существующей системе; однако эти функции покрываются, скорее, задачами управления логами;
- мониторинг безопасности системы; обеспечивает получение информации в реальном времени о состоянии, активности устройств и о событиях с контекстом безопасности, происходящих в устройствах, например о потенциальных атаках.

При построении системы управления средствами информационной безопасности предприятия возникает проблема организации взаимодействия и комплексирования традиционных систем управления КИС и систем управления информационной безопасностью. Для решения этой проблемы применяется два основных подхода.

Первый подход заключается в интеграции средств сетевого и системного управления с механизмами управления средствами защиты. Средства сетевого и системного управления ориентированы в первую очередь на управление сетью и информационными системами, т. е. поддерживают традиционные действия и услуги: управление учетными записями пользователей, управление ресурсами и событиями, маршрутизацию, производительность и т. п. Ряд компаний — Cisco Systems, IBM Tivoli Systems, Computer Associates, Hewlett Packard — пошли по пути интеграции механизмов управления средств защиты в традиционные системы управления. Однако такие комплексные системы управления часто отличаются высокой стоимостью и, кроме того, некоторые аспекты управления безопасностью остаются за пределами внимания этих систем.

Второй подход заключается в использовании средств, предназначенных для решения только задачи управления безопасностью. Например, Open Security Manager (OSM) от Check Point Software Technologies дает возможность централизованно управлять корпоративной политикой безопасности и инсталлировать ее на сетевые устройства по всей компании. Продукт OSM является одной из основных компонентов технологии OPSEC (Open Platform for Secure Enterprise Connectivity), разработанной компанией Check Point, он создает интерфейс для управления

устройствами сетевой безопасности различных производителей (например, Cisco, Bay, 3Com).

Для обеспечения безопасности информационных ресурсов предприятия средства защиты информации обычно размещаются непосредственно в корпоративной сети. Межсетевые экраны контролируют доступ к корпоративным ресурсам, отражая атаки злоумышленников извне, а шлюзы виртуальных частных сетей (VPN) обеспечивают конфиденциальную передачу информации через открытые глобальные сети, в частности Интернет. Для создания надежной эшелонированной защиты в настоящее время применяются также такие средства безопасности, как системы обнаружения и предотвращения вторжений IPS, средства контроля контента, антивирусные системы и др.

К сожалению, практически невозможно найти компанию-производителя, которая могла бы предоставить потребителю за приемлемую цену полный набор средств (от аппаратных до программных) для построения современной корпоративной информационной системы. Поэтому большинство КИС компаний обычно построены на основе программных и аппаратных средств, поставляемых различными производителями. Каждое из этих средств требует тщательного и специфического конфигурирования, отражающего взаимосвязи между пользователями и доступными им ресурсами.

Чтобы обеспечить в гетерогенной КИС надежную защиту информации, нужна рационально организованная система управления безопасностью КИС, которая обеспечила бы безопасность и правильную настройку каждого компонента КИС, постоянно отслеживала происходящие изменения, устанавливала «заплатки» на найденные в системе бреши, контролировала работу пользователей. Очевидно, что чем разнороднее информационная система, тем сложнее обеспечить управление ее безопасностью.

Опыт ведущих предприятий-производителей средств информационной безопасности показывает, что компания сможет успешно реализовать свою политику безопасности в распределенной корпоративной информационной системе, если управление безопасностью будет централизованным и не зависящим от используемых ОС и прикладных систем. Кроме того, система регистрации событий, происходящих в КИС (события НСД, изменение привилегий пользователей и т. д.), должна быть единой и позволять администратору составить полную картину происходящих в КИС изменений.

Для решения ряда задач управления безопасностью требуется применение единых вертикальных инфраструктур типа каталога X.500. Например, политика сетевого доступа требует знания идентификаторов пользователей. Эта информация нужна и другим приложениям, например в системе кадрового учета, в системе однократного доступа к приложениям (Single Sign-On) и т. д. Дублирование одних и тех же данных приводит к необходимости синхронизации, увеличению трудоемкости и возможной путанице. Поэтому, чтобы избежать такого дублирования, часто используют единые вертикальные инфраструктуры.

К таким вертикальным структурам, используемым различными пользовательскими подсистемами, работающими на разных уровнях OSI/ISO, относятся:

- инфраструктуры управления открытыми ключами PKI;
- каталоги (например, идентификаторов пользователей и других сведений о пользователях, необходимых, в системах управления доступом); каталоги часто используются не только как хранилища данных, в них также часто располагаются политики доступа, сертификаты, списки доступа и др.);
- системы аутентификации (обычно RADIUS, серверы TACACS, TACACS+);
- системы событийного протоколирования, мониторинга и аудита (следует отметить, что эти системы не всегда вертикальны, часто специализируются и работают автономно в интересах конкретных подсистем).

Учитывая, что методология централизованного управления достаточно полно отражает современные тенденции развития технологий обеспечения информационной безопасности КИС, российская компания НПО «Информзащита» разработала систему комплексного управления безопасностью КУБ. В системе КУБ реализуется оригинальная технология управления безопасностью. Особенность этой технологии заключается в том, что она предлагает полноценный организационный подход к решению проблемы управления безопасностью, поддержанный программными средствами. Использование этой технологии позволяет управлять безопасностью корпоративной информационной системы и обеспечить защиту нематериальных активов компании [87].

Основываясь на методологии централизованного управления, российская компания TrustWorks Systems разработала эффективную систему глобального управления безопасностью GSM (Global Security Management) для корпоративной информационной системы. Эта отечественная система управления информационной безопасностью КИС нашла широкое практическое применение и описывается в разделах 15.2, 15.3 и 15.5 данной главы.

Перейдем теперь к рассмотрению решений следующих задач управления безопасностью:

- управление обновлениями программных средств;
- управление конфигурациями объектов и субъектов доступа;
- управление учетными записями и правами доступа к активным сетевым устройствам, рабочим станциям и серверам.

Управление обновлениями программных средств

Регулярное обновление программных средств корпоративной информационной системы позволяет избежать угрозы эксплуатации злоумышленниками известных уязвимостей программного обеспечения. При этом увеличение сложности программного обеспечения

и количества компонентов приводит к тому, что практически ежедневно выходит несколько критичных обновлений, которые должны быть обязательно установлены на все рабочие станции и серверы предприятия.

Кроме того, каждое обновление должно быть предварительно проверено на совместимость с остальными программными средствами, используемыми на предприятии (например, предварительной установкой на тестовые рабочие станции).

Подсистемы управления обновлениями позволяют автоматизировать следующие задачи:

- автоматическое получение обновлений с сайтов производителей ПО;
- организацию централизованного хранилища обновлений;
- возможность назначения обновлений определенным рабочим станциям и серверам или группам рабочих станций и серверов;
- автоматическую установку выбранных обновлений на рабочие станции пользователей.

Управление конфигурациями

Централизованное управление конфигурацией рабочих станций, серверов, активного сетевого оборудования позволяет существенно сократить затраты на обеспечение актуальной конфигурации оборудования информационной системы предприятия.

Использование централизованного управления рабочими станциями и серверами позволяет:

- автоматически распространять приложения на рабочие станции и серверы;
- создавать типовые образы рабочих станций и серверов для быстрого ввода в эксплуатацию новых единиц техники;
- поддерживать соответствие локальных настроек политике безопасности организации.

Централизованное управление сетевым оборудованием позволяет:

- централизованно хранить конфигурации активного сетевого оборудования;
- распределять административные роли по типам и группам устройств;
- задавать высокоуровневые изменения сетевой инфраструктуры, которые будут автоматически преобразованы в изменения конфигураций конкретных сетевых устройств;
- осуществлять мониторинг сетевых устройств;
- производить откат неудачных изменений конфигурации.

Системы централизованного управления непосредственно зависят от систем централизованного управления учетными записями и правами доступа, а также систем администрирования доступа к сетевому оборудованию.

Разграничение доступа к сетевому оборудованию

Подсистема разграничения доступа к сетевому оборудованию включает в себя:

- централизованное управление доступом к сетевому оборудованию;
- разграничение доступа к командам сетевого оборудования.

Злонамеренные действия или ошибки администратора сетевого оборудования могут привести к нарушению конфиденциальности данных, передаваемых по корпоративной сети, или к другим инцидентам информационной безопасности.

В больших информационных системах очень сложно осуществлять контроль и управление административным доступом для каждого отдельного сетевого устройства. Это не позволяет в полной мере реализовать требования политики безопасности и предполагает большие трудозатраты со стороны системных администраторов, обусловленные необходимостью управления разрозненными локальными базами учетных записей.

Системы разграничения доступа к сетевому оборудованию, построенные на основе средств аутентификации авторизации и учета — AAA-серверов и средств делегирования административных полномочий, — позволяют решить задачи по разграничению доступа к конкретным командам управления, ведению журналов, а также по созданию централизованной базы учетных записей администраторов сетевого оборудования.

При организации доступа к сетевому оборудованию модель AAA подразумевает выполнение соответствующих процедур:

- аутентификация (Authentication) — процедура проверки данных учетной записи с целью установки соответствия пользователя множеству зарегистрированных субъектов доступа;
- авторизация (Authorization) — процедура установки полномочий пользователя и выделения ресурсов;
- учет (Accounting) — процедура учета действий, выполняемых пользователем на протяжении сеанса доступа.

AAA-серверы могут представлять собой как программные средства, так и программно-аппаратные комплексы.

В настоящее время наибольшую популярность получили следующие технологии, реализующие модель AAA: Remote Authentication in Dial-In User Service (RADIUS) и Terminal Access Controller Access-Control System (TACACS+).

Средства делегирования административных полномочий представляют собой отдельный класс средств разграничения административного доступа к сетевому оборудованию. Делегирование административных полномочий обеспечивается путем контроля административного доступа и ролевого разграничения доступа к конфигурационным командам.

Задача ролевого разграничения доступа к конфигурационным командам реализуется инструментальными комплексами в три этапа:

- сканирование активного сетевого оборудования на предмет выявления всех конфигурационных команд;

- анализ полученных результатов и создание политики безопасности с целью разграничения доступа к конфигурационным командам на основе ролей;
- создание конфигурации для ролевого разграничения доступа к командам.

Подсистема разграничения доступа к сетевому оборудованию может осуществлять взаимодействие с рядом других подсистем. В частности, взаимодействие с корпоративным LDAP-каталогом позволяет создать единое, в рамках организации, пространство учетных записей и упростить управление ими (рис. 15.1). Взаимодействие с системами мониторинга позволяет вести централизованный контроль за действиями администраторов на основе данных учета и предпринимать своевременные меры по предотвращению инцидентов информационной безопасности.

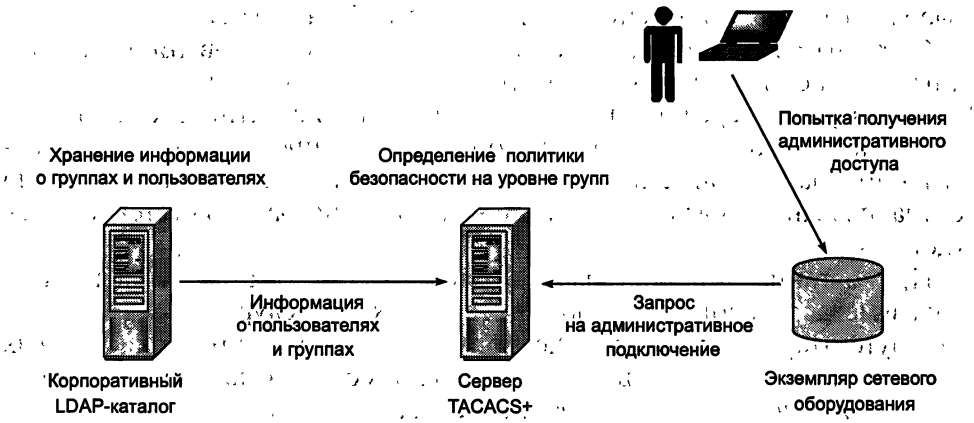


Рис. 15.1. Использование корпоративного LDAP-каталога для управления учетными записями

Аудит и мониторинг безопасности КИС рассматриваются в разделе 15.4.

Задачи управления криптосредствами, событийного протоколирования и ряд других решаются системой управления информационной безопасности с привлечением соответствующих подсистем комплексной системы защиты информации (см. раздел 7.3).

15.2. Архитектура управления информационной безопасностью КИС

Компания TrustWorks Systems разработала систему централизованного управления безопасностью КИС с применением глобальной и локальных политик безопасности. В основе централизованного управления безопасностью КИС лежит концепция глобального управления безопасностью GSM.

15.2.1. Концепция глобального управления безопасностью GSM

Концепция GSM позволяет построить комплексную систему управления и защиты информационных ресурсов предприятия со следующими свойствами:

- управление всеми существующими средствами защиты на базе политики безопасности предприятия, обеспечивающее целостность, непротиворечивость и полноту набора правил защиты для всех ресурсов предприятия (объектов политики безопасности) и согласованное исполнение политики безопасности средствами защиты, поставляемыми разными производителями;
- определение всех информационных ресурсов предприятия через единый (распределенный) каталог среды предприятия, который может актуализироваться как за счет собственных средств описания ресурсов, так и посредством связи с другими каталогами предприятия (в том числе по протоколу LDAP);
- централизованное, основанное на политике безопасности (Policy-based) управление локальными средствами защиты информации;
- строгая аутентификация объектов политики в среде предприятия с использованием токенов PKCS#11 и инфраструктуры открытых ключей PKI, включая возможность применения дополнительных локальных средств аутентификации LAS (по выбору потребителя);
- расширенные возможности администрирования доступа к определенным в каталоге ресурсам предприятия или частям всего каталога (с поддержкой понятий групп пользователей, доменов, департаментов предприятия), управление ролями как набором прав доступа к ресурсам предприятия, введение в политику безопасности элементов косвенного определения прав через атрибуты прав доступа (Credentials);
- обеспечение подотчетности (регистрация всех операций взаимодействий распределенных объектов системы в масштабах корпоративной сети) и аудита, мониторинга безопасности, тревожной сигнализации;
- интеграция с системами общего управления, инфраструктурными системами безопасности (PKI, LAS, IPS).

В рамках данной концепции термин «управление, основанное на политике безопасности PBM (Policy-based Management)» определяется как реализация набора правил управления, сформулированных для бизнес-объектов предприятия, которая гарантирует полноту охвата бизнес-области объектами и непротиворечивость используемых правил управления.

Система управления GSM, ориентированная на управление безопасностью предприятия на принципах PBM, удовлетворяет следующим требованиям:

- политика безопасности предприятия представляет собой логически и семантически связанную, формируемую, редактируемую и анализируемую как единое целое структуру данных;

- политика безопасности предприятия определяется в едином контексте для всех уровней защиты как единое целое сетевой политики безопасности и политики безопасности информационных ресурсов предприятия;
- для облегчения администрирования ресурсов и политики безопасности предприятия число параметров политики минимизируется.

Для того чтобы минимизировать число параметров политики, используются следующие приемы:

- групповые определения объектов безопасности;
- косвенные определения, например определения на основе верительных атрибутов;
- мандатное управление доступом (в дополнение к фиксированному доступу), когда решение о доступе определяется на основе сопоставления уровня доступа, которым обладает субъект, и уровня конфиденциальности (критичности) ресурса, к которому осуществляется доступ;

Система управления GSM обеспечивает разнообразные механизмы анализа политики безопасности за счет средств многокритериальной проверки соответствия политики безопасности формальным моделям концепции безопасности предприятия.

15.2.2. Глобальная и локальные политики безопасности

Согласно концепции GSM организация централизованного управления безопасностью КИС основана на следующих принципах:

- управление безопасностью корпоративной информационной системы должно осуществляться на уровне глобальной политики безопасности (ГПБ);
- ГПБ должна соответствовать бизнес-процессам компании. Для этого свойства безопасности объектов и требуемые сервисы безопасности должны быть описаны с учетом их бизнес-ролей в структуре компании;
- для отдельных средств защиты формируются локальные политики безопасности (ЛПБ). Трансляция ЛПБ должна осуществляться автоматически на основе анализа правил ГПБ и топологии защищаемой сети.

Глобальная политика безопасности корпоративной сети представляет собой конечное множество правил безопасности (Security Rules) — рис. 15.2, — которые описывают параметры взаимодействия объектов корпоративной сети в контексте информационной безопасности:

- необходимый для соединения сервис безопасности: правила обработки, защиты и фильтрации трафика;
- направление предоставления сервиса безопасности;
- правила аутентификации объектов;
- правила обмена ключами;

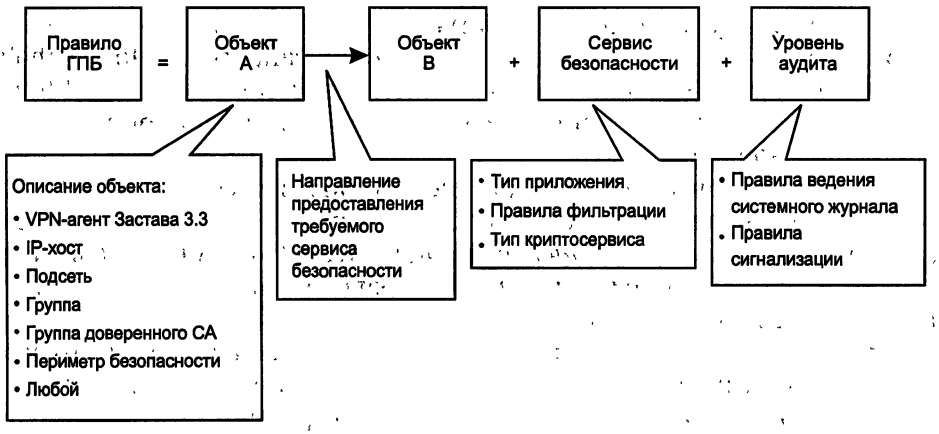


Рис. 15.2. Структура правила глобальной политики безопасности

- правила записи результатов событий безопасности в системный журнал;
- правила сигнализации о тревожных событиях и др.

При этом объектами ГПБ могут быть как отдельные рабочие станции и подсети, так и группы объектов, которые могут включать в себя целые структурные подразделения компании (например, отдел маркетинга или финансовый департамент) или даже отдельные компании (входящие, например, в холдинг). Политика безопасности для каждого объекта в группе автоматически реплицируется всем объектам группы.

Задачи защиты бизнес-объектов распределенной корпоративной системы можно сформулировать в терминах правил, поскольку сетевое взаимодействие можно представить как простую передачу информации между субъектом *Subj* и объектом *Obj* доступа на основе некоторого сетевого сервиса защиты *SecSrv*, настроенного при помощи параметров *P*. В результате глобальная политика безопасности предприятия представляется как набор правил вида

$$(Subj, Obj, SecSrv\ (P)).$$

При этом отсутствие правила для объекта *Obj* означает запрет любого доступа к данному *Obj*.

Для простоты определения целей безопасности предприятия в GSM предусмотрено два типа объектов, выступающих в качестве *Subj* и *Obj*. Это пользователь (*U*) и ресурс (*R*). Ресурс *R* может быть информационным (*IR*) или сетевым (*NR*).

Пользователь и ресурс могут выступать в любой из форм агрегации, поддерживаемых в системе: группы, домены, роли, департаменты, разделы каталога.

Пример: Правило (*U*, *IR*, *S*1) представляет собой правило защиты *S*1, обеспечиваемое при доступе пользователя *U* к информационному ресурсу *IR*. Правило (*IR*1, *IR*2, *S*2) означает разрешение сетевого взаимодействия двух информационных модулей (программ) с необходимостью обеспечения свойств защиты *S*2.

Политика по умолчанию для доступа к любому защищаемому объекту корпоративной системы представляет собой запретительное правило: *все, что не разрешено явно — запрещено.* Такое правило обеспечивает полноту защиты информации в сети предприятия и априорное отсутствие дыр в безопасности.

Чтобы обеспечить взаимодействие устройств в сети, для всех устройств сети создается и доставляется (в общем случае не по каналам сети) *стартовая конфигурация*, содержащая необходимые правила настройки устройств только для их централизованного управления, — стартовая политика безопасности устройства.

Правила ГПБ могут быть распространены как на сетевые взаимодействия, так и на функции контроля и управления самой системы.

Функционально правила ГПБ разбиты по группам:

- *правила VPN.* Правила данного тира реализуются при помощи протоколов IPSec; агентом исполнения данного правила является драйвер VPN в стеке клиентского устройства или шлюза безопасности (IP1, IP2, VPNRule);
- *правила пакетной фильтрации, включая NAT.* Эти правила обеспечивают пакетную фильтрацию типа stateful и stateless; исполнение этих правил обеспечивают те же агенты, что исполняют VPN-правила (IP1, IP2, PacketRule);
- *прокси-правила, включая антивирусную защиту «на лету».* Эти правила отвечают за фильтрацию трафика, передаваемого под управлением заданных прикладных протоколов; исполнительным агентом этих правил является прокси-агент, например (User, Protocol, ProxyRule) или (Application, Protocol, ProxyRule);
- *правила аутентифицированного/авторизованного доступа, включая правила однократного входа (Single Sign-On).* Управление доступом по схеме однократного входа обеспечивает данному пользователю работу на едином пароле или другой аутентификационной информации со многими информационными ресурсами; отсюда легко видеть, что символическая запись правила сетевого доступа легко распространяется на схему однократного входа (User, Application, Authentication Scheme). Правила этой группы могут комбинированно исполняться агентами различного уровня, от VPN-драйвера до прокси-агентов; кроме того, агентами исполнения таких правил могут быть системы аутентификации запрос—отклик и продукты третьих разработчиков;
- *правила, отвечающие за сигнализацию и событийное протоколирование.* Политика протоколирования может оперативно и централизованно управляться агентом протоколирования; исполнителями правил являются все компоненты системы.

Различие между правилами, реализующими глобальную политику безопасности ГПБ в сети, и правилами, реализующими локальную политику безопасности ЛПБ конкретного устройства, заключается в том, что в правилах группы ГПБ объекты и субъекты доступа могут быть распределены произвольным образом в пределах сети, а правила груп-

пы ЛПБ, включая субъекты и объекты ЛПБ, предназначены и доступны только в пределах пространства одного из сетевых устройств.

Набор правил ГПБ является логически целостным и семантически полным описанием политики безопасности в масштабах КИС, на основе которой может строиться локальная политика безопасности отдельных устройств.

Локальная политика безопасности. Любому средству защиты, реализующему какой-либо сервис информационной безопасности, необходима для выполнения его работы локальная политика безопасности ЛПБ, т. е. точное описание настроек для корректной реализации правил аутентификации пользователей, управления доступом, защиты трафика и др.

При традиционном подходе администратору приходится отдельно настраивать каждое средство защиты или реплицировать какие-то простейшие настройки на большое число узлов с последующей их корректировкой. Очевидно, что это неизбежно приводит к большому числу ошибок администрирования и, как следствие, к существенному снижению уровня защищенности корпоративной сети.

После формирования администратором глобальной политики безопасности, центр управления на основе интерпретации ГПБ автоматически вычисляет и, если это необходимо, корректирует отдельные ЛПБ для каждого средства защиты и автоматически загружает необходимые настройки в управляющие модули соответствующих средств защиты.

В целом локальная политика безопасности сетевого устройства включает в себя полный набор правил разрешенных соединений данного устройства, исполняемых для обеспечения какой-либо информационной услуги с требуемыми свойствами защиты информации.

15.3. Функционирование системы управления информационной безопасностью КИС

Структурно-продуктная линия системы управления GSM подразделяется на агентов безопасности, центр управления и консоль управления. Общая структурная схема решения показана на рис. 15.3.

15.3.1. Назначение основных средств защиты

Агент безопасности (Trusted Agent), установленный на *персональном компьютере клиента*, ориентирован на защиту индивидуального пользователя, выступающего, как правило, клиентом в приложениях клиент/сервер.

Агент безопасности, установленный на *сервере приложений*, ориентирован на обеспечение защиты серверных компонентов распределенных приложений.

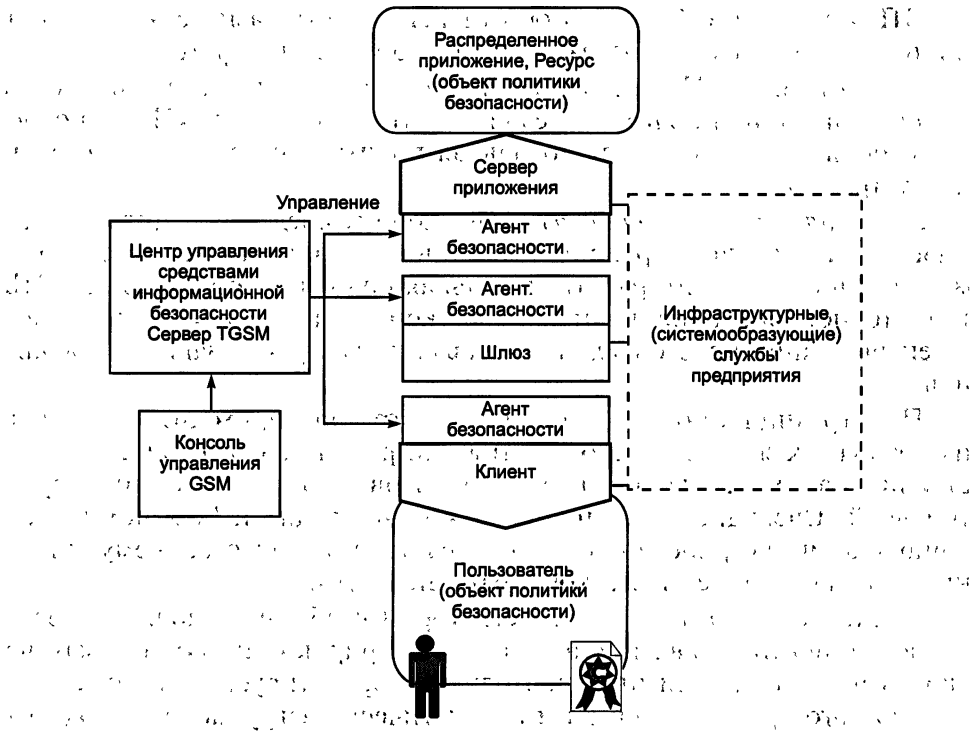


Рис. 15.3. Общая структурная схема системы управления средствами информационной безопасности

Агент безопасности, установленный на *шлюзовом компьютере*, обеспечивает развязку сегментов сети внутри предприятия или между предприятиями.

Центр управления (Trusted GSM Server) обеспечивает описание и хранение глобальной политики безопасности в масштабах сети, трансляцию глобальной политики в локальные политики безопасности устройств защиты, загрузку устройств защиты и контроль состояний всех агентов системы. Для организации распределенной схемы управления безопасности предприятия в системе GSM предусматривается установка нескольких (до 65 535) серверов GSM.

Консоль управления (Trusted GSM Console) предназначена для организации рабочего места администратора (администраторов) системы. Для каждого из серверов GSM может быть установлено несколько консолей, каждая из которых настраивается согласно ролевым правам каждого из администраторов системы GSM.

Локальный агент безопасности представляет собой программу, размещаемую на оконечном устройстве (клиенте, сервере, шлюзе) и выполняющую следующие функции защиты:

- аутентификацию объектов политики безопасности, включая интеграцию различных сервисов аутентификации;
- определение пользователя в системе и событий, связанных с данным пользователем;

- обеспечение централизованного управления средствами безопасности и контроля доступа;
- управление ресурсами в интересах приложений, поддержку управления доступом к ресурсам прикладного уровня;
- защиту и аутентификацию трафика;
- фильтрацию трафика;
- событийное протоколирование, мониторинг, тревожную сигнализацию.

Дополнительные функции агента безопасности (разрабатываются в составе решения GSM):

- поставка криптосервиса (Multiple Concurrent Pluggable Modules);
- управление параметрами Single Sign-On (как подзадача аутентификации пользователей);
- сервис в интересах защищенных приложений (криптосервис, сервис доступа к PKI, доступ к управлению безопасностью);
- сжатие трафика (IPcomp, Pluggable Module);
- управление резервированием сетевых ресурсов (QoS);
- функции локального агента сетевой антивирусной защиты.

Центральным элементом локального агента является процессор локальной политики безопасности (LSP Processor), интерпретирующий локальную политику безопасности и распределяющий вызовы между остальными компонентами.

15.3.2. Защита ресурсов

Аутентификация и авторизация доступа. В рамках решения реализуется ряд различных по функциональности схем аутентификации, каждая из которых включает тип аутентификации и способ (механизм) идентификации объектов.

Для выбора типа аутентификации предусмотрены следующие возможности: аутентификация пользователя при доступе к среде GSM или локальной операционной системе, аутентификация пользователя при доступе в сеть (сегмент сети), взаимная сетевая аутентификация объектов (приложение-приложение). Для выбора способа идентификации предусмотрены следующие варианты, предполагающие их любое совместное использование: токен (смарт-карта), пароль, внешняя аутентификация.

Контроль доступа при сетевых взаимодействиях. При инициализации защищенного сетевого соединения от локальной операционной системы или при получении запроса на установление внешнего соединения локальные агенты безопасности на концах соединения (и/или на промежуточном шлюзе) обращаются к локальной политике безопасности устройства и проверяют, разрешено ли установление данного соединения. В случае если такое соединение разрешено, обеспечивается требуемый сервис защиты данного соединения, если запрещено — сетевое соединение не предоставляется.

Контроль доступа на уровне прикладных объектов. Для незащищенных распределенных приложений в GSM обеспечивается сервис разграничения прав доступа на уровне внутренних объектов данного приложения. Контроль доступа на уровне объектов прикладного уровня обеспечивается за счет применения механизма прокси. Прокси разрабатывается для каждого прикладного протокола. Предустановленным является протокол HTTP.

Для построения распределенной схемы управления и снижения загрузки сети в GSM используется архитектура распределенных прокси-агентов Lightweight Proxy (Proxy Module в составе Trusted Agent), каждый из которых:

- имеет абстрактный универсальный интерфейс, обеспечивающий модульное подключение различных прокси-фильтров;
- имеет интерфейс к системе управления, но использует временный кэш для управления параметрами фильтрации;
- фильтрация управляется обобщенными правилами типа:
  - аутентифицировать субъект *X* в приложении-объекте *Y*;
  - разрешить доступ субъекту *X* к объекту *Y* с параметрами *P*;
  - запретить доступ субъекту *X* к объекту *Z*;
- семантика правил управления прокси-фильтром и описания субъектов и объектов доступа зависят от конкретного прикладного протокола, однако центр управления имеет возможность регистрировать прокси-фильтры и обеспечивать управление ими в контексте общей глобальной политики безопасности.

Прокси-агент может быть установлен на шлюзе безопасности, непосредственно на сервере, исполняющем контролируемые приложения, и на клиентском месте системы.

15.3.3. Управление средствами защиты

Важнейшим элементом решения TrustWorks является централизованная, основанная на политике (Policy-based) система управления средствами сетевой и информационной безопасности масштаба предприятия. Эта система обеспечивает следующие качественные потребительские характеристики:

- высокий уровень защищенности системы управления (путем выделения защищенного периметра управления внутри сети предприятия);
- расширяемость системы управления информационной безопасностью;
- высокий уровень надежности системы управления и ключевых ее компонентов;
- интеграция с корпоративными системами общего сетевого и информационного управления;
- простая, интуитивно воспринимаемая, эргономичная и инфраструктурная среда описания, формирования, мониторинга и диаг-

ностики политики безопасности масштаба предприятия (Enterprise Level Policy-based Management).

Управление осуществляется специальным программным обеспечением администратора — консолью управления. Количество и функции каждой из установленных в системе ПО консолей управления задаются главным администратором системы в зависимости от организационной структуры предприятия. Для назначения функций каждого из рабочих мест консоли управления используется ролевой механизм разграничения прав по доступу к функциям управления (менеджмента) системы.

Функции управления GSM. В зависимости от вида управляемых объектов набор управляющих функций в GSM можно условно разбить на три категории:

- управление информационным каталогом;
- управление пользователями и правами доступа;
- управление правилами ГПБ.

Функции управления информационным каталогом определяют информационную составляющую GSM:

- формирование разделов каталога;
- описание услуг каталога;
- назначение и контроль сетевых ресурсов, требуемых для выполнения услуги;
- регистрация описания услуги;
- контроль состояния услуг или разделов каталога услуг;
- мониторинг исполнения услуг;
- подготовка и пересылка отчетов (протоколов) по состоянию каталога.

Для управления правами доступа пользователей системы к услугам (информационным или сетевым ресурсам) GSM обеспечивает следующие функции:

- формирование групп пользователей по ролям и/или привилегиям доступа к услугам системы;
- формирование иерархических агрегаций пользователей по административным, территориальным или иным критериям (домены и/или департаменты);
- формирование ролей доступа пользователей к услугам (информационным или сетевым ресурсам);
- назначение уровней секретности для услуг и пользователей системы (поддержка мандатного механизма разграничения прав);
- назначение фиксированных прав доступа группам, ролям, агрегациям пользователей или отдельным пользователям системы к информационным или сетевым ресурсам системы;
- подготовка и пересылка отчетов (протоколов) по доступу пользователей к услугам системы;
- подготовка и пересылка отчетов (протоколов) по работе администраторов системы.

Правила ГПБ ставят в соответствие конкретные свойства защиты (как для сетевых соединений, так и для доступа пользователей к ин-

формационным услугам) предустановленным уровням безопасности системы. Контроль за соблюдением правил ГПБ выполняет специальный модуль в составе сервера системы — *Security Policy Processor*, — обеспечивающий следующие функции системы:

- определение каждого из уровней безопасности набором параметров защиты соединений, схемы аутентификации и разграничения прав;
- назначение уровней безопасности конкретным услугам или разделам каталога услуг;
- назначение уровней безопасности пользователям или любым агрегациям пользователей системы (группам, ролям, доменам, департаментам);
- контроль за целостностью ГПБ (полнотой правил);
- вычисление политик безопасности ЛПБ локальных устройств защиты — агентов безопасности — и контроль их исполнения;
- контроль за исполнением ГПБ по различным критериям;
- подготовка и пересылка отчетов (протоколов) по состоянию системы и всех попыток нарушения ГПБ.

Каждый из администраторов системы аутентифицируется и работает с системой через консоль управления согласно предустановленным для него правам (на каталог ресурсов или его часть, на определенный ролями набор функций управления, на группы или другие наборы пользователей). Все действия любого из администраторов протоколируются и могут быть попарно контролируемы.

15.4. Аудит и мониторинг безопасности КИС

Для организаций, компьютерные сети которых насчитывают не один десяток компьютеров, функционирующих под управлением различных операционных систем, на первое место выступает задача управления множеством разнообразных защитных механизмов в таких гетерогенных корпоративных сетях. Сложность сетевой инфрастуктуры, многообразие данных и приложений приводят к тому, что при реализации системы информационной безопасности за пределами внимания администратора безопасности могут остаться многие угрозы. Поэтому необходимо осуществление регулярного аудита и постоянного мониторинга безопасности информационных систем.

15.4.1. Аудит безопасности информационной системы

Понятие аудита безопасности

Аудит представляет собой независимую экспертизу отдельных областей функционирования предприятия. Одной из составляющих аудита предприятия является аудит безопасности его информационной сис-

темы (ИС). *Аудит безопасности ИС* — системный процесс получения и оценки объективных данных о текущем состоянии защищенности информационной системы, действиях и событиях происходящих в ней, устанавливающий уровень их соответствия определенному критерию.

В настоящее время актуальность аудита безопасности ИС резко возросла, это связано с увеличением зависимости организаций от информации и ИС. Возросла уязвимость ИС за счет повышения сложности элементов ИС, появления новых технологий передачи и хранения данных, увеличения объема программного обеспечения. Расширился спектр угроз для ИС из-за активного использования предприятиями открытых глобальных сетей для передачи сообщений и транзакций.

Аудит безопасности ИС дает возможность руководителям и сотрудникам организаций получить ответы на приведенные ниже вопросы, а также наметить пути решения обнаруженных проблем:

- как оптимально использовать существующую ИС при развитии бизнеса;
- как решаются вопросы безопасности и контроля доступа;
- как установить единую систему управления и мониторинга ИС;
- когда и как необходимо провести модернизацию оборудования и ПО;
- как минимизировать риски при размещении конфиденциальной информации в ИС организации.

На эти и другие подобные вопросы нельзя мгновенно дать однозначный ответ. Достоверную и обоснованную информацию можно получить, только рассматривая все взаимосвязи между проблемами. Проведение аудита позволяет оценить текущую безопасность ИС, оценить риски, прогнозировать и управлять их влиянием на бизнес-процессы организации, корректно и обоснованно подойти к вопросу обеспечения безопасности информационных ресурсов организации.

Целями проведения аудита безопасности ИС являются:

- оценка текущего уровня защищенности ИС;
- локализация узких мест в системе защиты ИС;
- анализ рисков, связанных с возможностью осуществления угроз безопасности в отношении ресурсов ИС;
- выработка рекомендаций по внедрению новых и повышению эффективности существующих механизмов безопасности ИС;
- оценка соответствия ИС существующим стандартам в области информационной безопасности.

В число дополнительных задач аудита ИС могут также входить выработка рекомендаций по совершенствованию политики безопасности организации и постановка задач для ИТ персонала, касающихся обеспечения защиты информации.

К настоящему времени подход к проведению аудита ИС приобрел стандартизованные формы. Крупные и средние аудиторские компании образовали ассоциации — союзы профессионалов в области аудита ИС, — которые занимаются созданием и сопровождением стандартов аудиторской деятельности в сфере ИТ.

Проведение аудита безопасности информационных систем

Работы по аудиту безопасности ИС включают в себя ряд последовательных этапов, которые в целом соответствуют этапам проведения комплексного ИТ-аудита автоматизированной системы:

- инициирование процедуры аудита;
- сбор информации аудита;
- анализ данных аудита;
- выработка рекомендаций;
- подготовка аудиторского отчета.

Последовательность выполнения этапов аудита безопасности ИС показана на рис. 15.4.

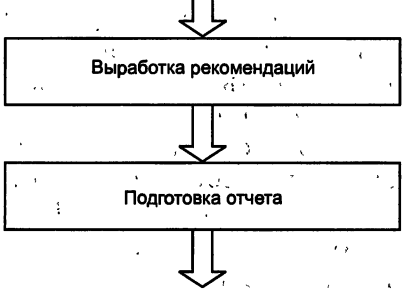


Рис. 15.4. Последовательность этапов проведения аудита ИС

Рассмотрим эти этапы подробнее [4].

Инициирование процедуры аудита. Аудит проводится по инициативе руководства компании, которое в данном вопросе является основной заинтересованной стороной. Аудит представляет собой комплекс мероприятий, в которых помимо самого аудитора оказываются задействованными представители большинства структурных подразделений компании. Действия всех участников этого процесса должны быть четко скоординированы. Поэтому на этапе инициирования процедуры аудита должны быть решены соответствующие организационные вопросы, связанные с подготовкой и утверждением плана проведения аудита, закреплением прав и обязанностей аудитора и т. п.

Сбор информации аудита. Этап сбора информации аудита является наиболее сложным и длительным. Это связано с необходимостью плот-

ного взаимодействия аудитора со многими должностными лицами организации. Компетентные выводы относительно положения дел в компании с информационной безопасностью могут быть сделаны аудитором только при наличии всех необходимых исходных данных для анализа.

Получение информации об организации, функционировании и текущем состоянии ИС осуществляется аудитором в ходе специально организованных интервью с ответственными лицами компании, путем изучения технической и организационно-распорядительной документации, а также исследования ИС с использованием специализированного программного инструментария. Когда все необходимые данные по ИС, включая документацию, подготовлены, можно переходить к их анализу.

Анализ данных аудита. Проведение анализа является наиболее ответственной частью проведения аудита ИС. Используемые аудиторами методы анализа данных определяются выбранными подходами к проведению аудита, которые могут существенно различаться.

Первый подход базируется на анализе рисков. Цель анализа рисков состоит в том, чтобы выявить существующие риски и оценить их величину (дать им качественную либо количественную оценку). Опираясь на методы анализа рисков, аудитор определяет для обследуемой ИС индивидуальный набор требований безопасности, в наибольшей степени учитывающий особенности данной ИС, среды ее функционирования и существующие в данной среде угрозы безопасности.

Второй подход опирается на использование стандартов информационной безопасности. Стандарты определяют базовый набор требований безопасности для широкого класса ИС, который формируется в результате обобщения мировой практики. Стандарты могут определять разные наборы требований безопасности в зависимости от уровня защищенности ИС, который требуется обеспечить, ее принадлежности (коммерческая организация либо государственное учреждение), а также назначения (финансы, промышленность, связь и т. п.). От аудитора в данном случае требуется правильно определить набор требований стандарта, соответствие которым требуется обеспечить для данной ИС. Необходима также методика, позволяющая оценить это соответствие. Из-за своей простоты и надежности описанный подход наиболее распространен на практике. Он позволяет при минимальных затратах ресурсов делать обоснованные выводы о состоянии ИС.

Третий подход предполагает комбинирование первых двух подходов. Базовые требования безопасности, предъявляемые к ИС, определяются стандартом. Дополнительные требования, учитывающие особенности функционирования данной ИС, формируются на основе анализа рисков. Этот подход значительно проще первого, так как бóльшая часть требований безопасности уже определена стандартом, и в то же время он лишен недостатков второго подхода, заключающихся в том, что требования стандарта могут не учитывать специфики обследуемой ИС.

Выработка рекомендаций. Рекомендации, выдаваемые аудитором, определяются особенностями обследуемой ИС, состоянием дел с ин-

формационной безопасностью и степенью детализации, используемой при проведении аудита. Рекомендации аудитора должны быть конкретными и применимыми к данной ИС, экономически обоснованными, аргументированными (подкрепленными результатами анализа) и ранжированными по степени важности.

Подготовка отчетных документов. Аудиторский отчет является основным результатом проведения аудита. Его качество характеризует качество работы аудитора. Отчет должен содержать описание целей проведения аудита, характеристику обследуемой ИС, указание границ проведения аудита и используемых методов, результаты анализа данных аудита, выводы, обобщающие эти результаты и содержащие оценку уровня защищенности АС или соответствие ее требованиям стандартов, и, конечно, рекомендации аудитора по устранению существующих недостатков и совершенствованию системы защиты.

Результаты проведения аудита. Результаты аудита ИС организации можно разделить на три основные группы:

- организационные — планирование, управление, документооборот функционирования ИС;
- технические — сбои, неисправности, оптимизация работы элементов ИС, непрерывное обслуживание, создание инфраструктуры и т. д.;
- методологические — подходы к решению проблемных ситуаций, управлению и контролю, общая упорядоченность и структуризация.

Проведенный аудит позволяет обоснованно создавать следующие документы:

- политику безопасности ИС организации;
- методологию работы и доводки ИС организации;
- долгосрочный план развития ИС;
- план восстановления ИС в чрезвычайной ситуации.

15.4.2. Мониторинг безопасности системы

Функции мониторинга безопасности информационной системы выполняет подсистема мониторинга и управления инцидентами информационной безопасности (см. главу 7). Подсистема мониторинга анализирует настройки элементов защиты операционных систем на рабочих станциях и серверах, в базах данных, а также топологию сети; ищет незащищенные или неправильные сетевые соединения; анализирует настройки межсетевых экранов.

Управление инцидентами информационной безопасности является реагированием системы управления безопасностью на меняющиеся условия и может быть различным по форме, например:

- пассивным, т. е. реализовывать лишь уведомление системы сетевого управления по протоколу SNMP или администратора по электронной почте либо на пейджер;

- активным, т. е. самостоятельно автоматически завершать сессию с атакующим узлом либо пользователем, реконфигурировать настройку межсетевого экрана или таких сетевых устройств, как маршрутизаторы.

В функции системы управления безопасностью входит выработка рекомендаций администратору по устранению обнаруженных уязвимостей в сетях, приложениях или иных компонентах информационной системы организации.

Важным вопросом является организация взаимодействия систем мониторинга (активного аудита) и общего управления [3, 6]. Активный аудит выполняет типичные управляющие функции — анализ данных об активности в информационной системе, отображение текущей ситуации, автоматическое реагирование на подозрительную активность. Сходным образом функционирует система сетевого управления. Активный аудит и общее управление целесообразно интегрировать, используя общие программно-технические и организационные решения. В эту интегрированную систему может быть включен и контроль целостности, а также агенты другой направленности, отслеживающие специфические аспекты поведения ИС (рис. 15.5).

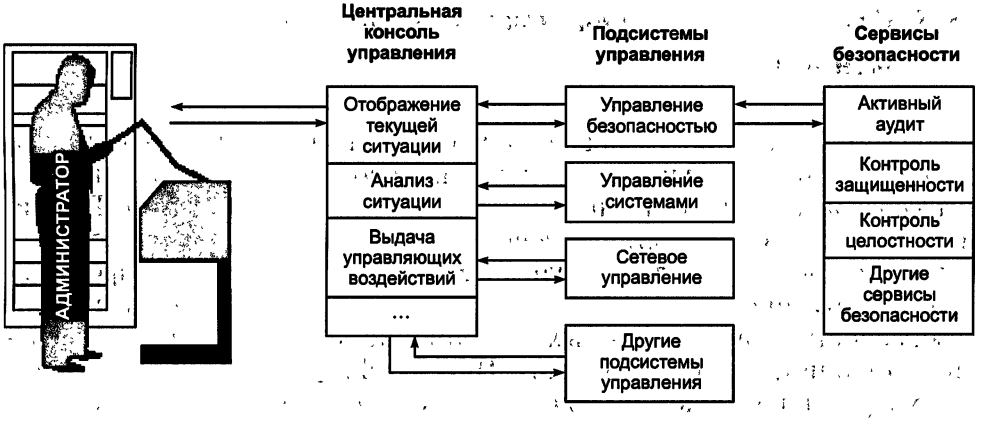


Рис. 15.5. Интеграция сервисов безопасности и системы управления

С логической точки зрения можно считать, что существует центральная консоль управления, куда стекаются данные от систем мониторинга (активного аудита), контроля целостности, контроля систем и сетей по другим аспектам. На этой консоли отображается текущая ситуация, с нее, автоматически или вручную, выдаются управляющие команды. По техническим или организационным причинам эта консоль может быть физически реализована в виде нескольких рабочих мест (с выделением, например, места администратора безопасности).

Один из известных специалистов в области информационной безопасности, Маркус Ранум (Markus Ranum), считает, что действия по обнаружению ошибок, вторжений или отказов являются аспектами единой проблемы управления сетями [3, 6]. В частности, продукт для ак-

тивного аудита NFR (Network Flight Recorder) М. Ранум рассматривает как компонент системы сетевого управления.

Использование модели адаптивного управления безопасностью сети дает возможность контролировать практически все угрозы и своевременно реагировать на них, позволяя не только устранить уязвимости, которые могут привести к реализации угрозы, но и проанализировать условия, приводящие к появлению уязвимостей.

Примерами систем, осуществляющих мониторинг и управление инцидентами информационной безопасности, являются такие программные продукты компании IBM, как IBM Tivoli Security Operations Manager (TSOM) и IBM Tivoli Security Information and Event Manager (TSIEM). TSOM обеспечивает оперативный мониторинг событий безопасности и предназначен в основном для снижения рисков и угроз, исходящих от внешних нарушителей и технологий (см. раздел 15.5.3). TSIEM осуществляет сбор и анализ информации, полученной от различных средств защиты информации, а также анализ нарушений безопасности, используя корреляцию событий безопасности, выявление на их основе тенденций и прогнозирование возможных в будущем атак.

15.5. Обзор современных систем управления безопасностью

Задачи управления безопасностью корпоративных информационных систем стали актуальными в эпоху массового распространения клиент/серверных технологий и децентрализованных вычислений. Принимая этот вызов времени, поставщики стали разрабатывать продукты, позволяющие решать задачи управления безопасностью распределенных информационных систем. Лидерами на рынке средств управления безопасностью распределенных информационных систем являются такие компании, как Cisco Systems, IBM Tivoli, Check Point и др. Ниже рассматриваются некоторые конкретные реализации средств управления безопасностью.

15.5.1. Централизованное управление безопасностью, реализованное в продуктах «ЗАСТАВА»

Принцип централизованного управления безопасностью корпоративной сети, разработанный компанией TrustWorks Systems (см. раздел 15.2) и реализованный в продуктах «ЗАСТАВА» компании ЭЛВИС+, основывается на следующих концептуальных положениях:

- управление безопасностью корпоративной сети должно осуществляться на уровне глобальной политики безопасности — наборе правил безопасности для сколь угодно сложного множества взаимодействий между разнообразными объектами корпоративной

сети, а также между объектами корпоративной сети и внешними объектами;

- ГПБ должна максимальным образом соответствовать бизнес-процессам компании; для этого должен существовать способ описания свойств безопасности объектов и требуемых для их реализации сервисов безопасности, основанный на их бизнес-ролях в структуре компании;
- формирование локальных политик безопасности для отдельных средств защиты и их трансляция должны осуществляться автоматически на основе анализа правил ГПБ и топологии защищаемой сети с обязательной автоматической проверкой их корректности, целостности и непротиворечивости ГПБ (рис. 15.6).

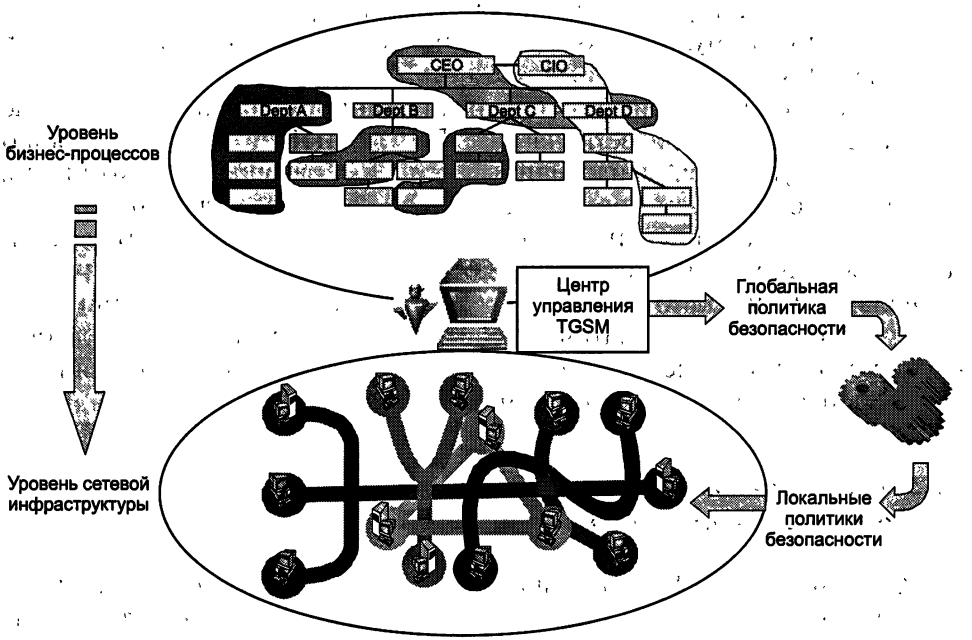


Рис. 15.6. Структура централизованного управления безопасностью сети

Объектами глобальной политики безопасности могут быть как отдельные рабочие станции и подсети, так и группы объектов, которые могут включать в себя целые структурные подразделения компании (например, отдел маркетинга или финансовый департамент) или даже отдельные компании (входящие, например, в холдинг). Администратору безопасности не нужно заботиться о формировании политики безопасности для каждого объекта в группе — заданная политика автоматически реплицируется всем объектам группы.

Локальная политика безопасности необходима для нормального функционирования любого средства защиты, реализующего какой-либо сервис информационной безопасности. Локальная политика безопасности представляет собой точное описание настроек средства защиты

для корректной реализации правил аутентификации пользователей, управления доступом, защиты трафика и др.

Решение на базе VPN «ЗАСТАВА» реализует эффективный подход к проблеме обеспечения безопасности корпоративной сети: после формирования ГПБ администратором центр управления TGSM на основе ее интерпретации автоматически вычисляет и, если это необходимо, корректирует отдельные ЛПБ для каждого средства защиты и автоматически загружает необходимые настройки в управляющие модули соответствующих средств защиты:

- в автоматическом режиме по протоколу PMP (Policy Management Protocol), являющемуся стандартным расширением протокола IKE в виде сообщения в формате PKCS#7;
- в ручном режиме путем выдачи ЛПБ на PKCS#11-совместимый идентификатор пользователя (смарт-карта, USB-токен, программный эмулятор токена на дискете или жестком диске) в формате PKCS#7.

Таким образом, принцип централизованного управления безопасностью корпоративной сети на базе ГПБ и ЛПБ позволяет формировать целостную и непротиворечивую политику безопасности компании, независимую от форматов и содержания настроек отдельных средств защиты, реализующих данную политику. Для этого используется патентованная технология TrustWorks, которая позволяет интерпретировать правила безопасности ГПБ и ставить их в соответствие с топологией защищаемой сети, автоматически вычислять и предоставлять локальные политики безопасности всем узлам, где реализуется заданная политика безопасности корпоративной сети.

15.5.2. Программные средства компании Cisco для управления безопасностью сетей

Компания Cisco Systems, признанный лидер в области сетевых решений, предлагает также широкий выбор продуктов в области обеспечения информационной безопасности — от межсетевых экранов и систем предотвращения атак до средств персональной защиты рабочих станций и систем централизованного управления средствами защиты.

Система управления Cisco Security Manager

Cisco Security Manager (CSM) — система централизованного управления всеми средствами защиты компании Cisco, пришедшая на смену CiscoWorks VMS. Отличительными особенностями CSM являются поддержка большего числа устройств защиты, различные формы представления информации, механизмы обнаружения несоответствий в политике безопасности, автоматизация рутинных задач и т. д.

Основные возможности:

- графический интерфейс управления;

- различные формы представления информации: в виде топологии сети, географической карты, таблицы правил;
- обнаружение конфликтов в правилах политики безопасности;
- обнаружение правил, не влияющих на защищенность сети;
- группирование объектов;
- клонирование настроек для ускорения внедрения средств защиты;
- поддержка иерархии и наследования политик безопасности;
- откат к предыдущей конфигурации;
- импорт настроек из различных источников;
- инвентаризация политик для уже внедренных средств защиты;
- автоматическая настройка VPN-туннелей для различных топологий (Site-to-Site, Hub & Spoke, Partial Mesh, Full Mesh и т. д.);
- управление механизмами отказоустойчивости, балансировки нагрузки и контроля качества обслуживания для управляемых средств защиты;
- ролевое управление административным доступом с помощью Cisco Secure ACS;
- автоматическое обновление средств защиты;
- управление ACL и VLAN на Catalyst 6500 и Cisco 7600;
- интеграция с Cisco MARS для корреляции сетевых событий и заданных правил на МСЭ, что помогает более быстро принимать решения и повышает работоспособность сети;
- управление и конфигурирование политик безопасности на МСЭ Cisco, включая устройства Cisco ASA 5500, Cisco PIX, модули на Cisco Catalyst 6500;
- обеспечение высокой доступности;
- контроль административных действий на защитных устройствах;
- управление SSL VPN.

Программно-аппаратный комплекс Cisco MARS

Программно-аппаратный комплекс Cisco Monitoring, Analysis and Response System (MARS) предназначен для управления противодействием угрозам безопасности. В качестве источников информации о них могут выступать сетевое оборудование (маршрутизаторы и коммутаторы), средства защиты (межсетевые экраны, антивирусы, системы обнаружения атак и сканеры безопасности), журналы регистрации ОС (Solaris, Windows NT/2000/2003, Linux) и приложений (СУБД, веб- и т. д.), а также сетевой трафик (например, Cisco Netflow). Cisco MARS поддерживает решения различных производителей — Cisco, ISS, Check Point, Symantec, NetScreen, Extreme, Snort, McAfee, eEye, Oracle, «Майкрософт» и т. д. Механизм ContextCorrelationTM позволяет проанализировать и сопоставить события от разнородных средств защиты.

Визуализация их на карте сети в реальном времени достигается с помощью механизма SureVectorTM. Данные механизмы позволяют отобразить путь распространения атаки в режиме реального времени. Ав-

томатическое блокирование обнаруженных атак достигается с помощью механизма AutoMitigateTM, который позволяет реконфигурировать различные средства защиты и сетевое оборудование.

Основные возможности:

- обработка до 10 000 событий в секунду или свыше 300 000 событий Netflow в секунду;
- возможность создания собственных правил корреляции;
- уведомление об обнаруженных проблемах по электронной почте, SNMP, через Syslog и на пейджер;
- визуализация атаки на канальном и сетевом уровнях;
- поддержка Syslog, SNMP, RDEP, SDEE, NetFlow, системных и пользовательских журналов регистрации в качестве источников информации;
- возможность подключения собственных средств защиты для анализа;
- эффективное отсечение ложных срабатываний и шума, а также обнаружение атак, пропущенных отдельными средствами защиты;
- обнаружение аномалий с помощью протокола NetFlow;
- создание и автоматическое обновление карты сети, включая импорт из CiscoWorks и других систем сетевого управления;
- поддержка IOS 802.1x, NAC (фаза 2);
- мониторинг механизмов защиты коммутаторов (Dynamic ARP Inspection, IP Source Guard и т. д.);
- интеграция с Cisco Security Manager (CSM Policy Lookup);
- интеграция с системами управления инцидентами с помощью XML Incident Notification;
- слежение за состоянием контролируемых устройств;
- интеграция с Cisco Incident Control System (ICS);
- аутентификация на RADIUS-сервере;
- мониторинг работоспособности компонентов Cisco MARS;
- Syslog forwarding;
- динамическое распознавание новых сигнатур атак на Cisco IPS и загрузка их в Cisco MARS.

Cisco IP Solution Center (ISC)

Cisco IP Solution Center (ISC) — платформа централизованного управления сетевой инфраструктурой крупных компаний и сервис-провайдеров. В том числе ISC управляет и решениями по информационной безопасности — механизмами построения VPN (ЛВС—ЛВС, удаленный доступ, EasyVPN, DMVPN), межсетевыми экранами, сетевой трансляцией адресов (NAT) и качеством сервиса (QoS) на маршрутизаторах с Cisco IOS, МСЭ Cisco Pix и устройствах VPN Concentrator. Эту задачу решает специальное приложение — ISC Security Management.

ISC Security Management предоставляет возможность управления жизненным циклом средств защиты, начиная от создания политик

безопасности, активации и аудита защитной услуги и заканчивая оценкой качества предоставления защитной услуги и реконфигурацией используемой политики. Все это позволяет обеспечивать безопасность инфраструктуры без нарушения ее доступности и устойчивости.

15.5.3. Продукты компании IBM для управления средствами безопасности

Управление безопасностью имеет много аспектов, и только при комплексном подходе к решению этой задачи можно создать действительно безопасную среду функционирования ИС предприятия. Два подразделения — IBM Tivoli и IBM Internet Security Systems (IBM ISS) — компании IBM предлагают средства защиты и управления для обеспечения безопасности ИТ-инфраструктуры предприятий.

Продукты IBM Tivoli для управления средствами безопасности

На рис. 15.7 представлена информация о функциональности продуктов IBM Tivoli для обеспечения безопасности КИС [7].

При формировании стратегии безопасности предприятия подразделение IBM Tivoli выделяет в качестве приоритетных задач:

- выработку политики доступа к ресурсам или данным и реализацию ее на всех уровнях корпоративной инфраструктуры;
- комплексную защиту от несанкционированного проникновения в сеть, вирусных атак и других угроз вторжения извне и изнутри.

Для решения этих проблем обеспечения безопасности в продуктах IBM Tivoli предусмотрена реализация нескольких функций.

Первая функция — *управление идентификацией (Identity Management)* — включает управление процессами аутентификации и авторизации пользователей по отношению к информационным ресурсам предприятия.

Вторая функция — *управление доступом (Access Management)* к информационным ресурсам предприятия.

Третья функция — *централизованное управление и реагирование на различные угрозы и попытки вторжения, направленные на информационные ресурсы предприятия (Security Operations Manager).* Функция дает возможность определять вторжение извне и изнутри и автоматически запускать превентивные процедуры.

Четвертая функция — *создание вычислительной и коммуникационной основы (Management Framework)* для функционирования всех модулей обеспечения безопасности.

Для реализации перечисленных функций подразделение IBM Tivoli предлагает следующие продукты:

- IBM Tivoli Identity Manager;
- IBM Tivoli Access Manager;

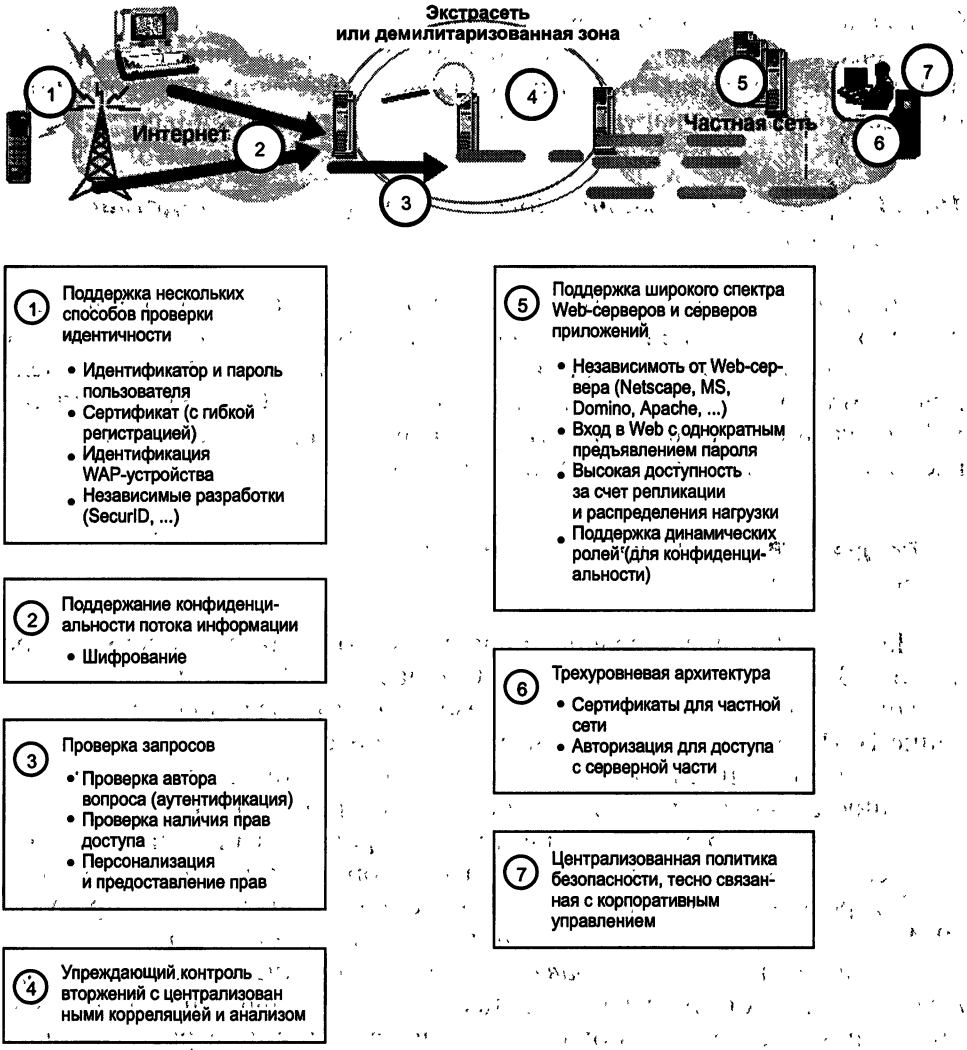


Рис. 15.7. Функциональность продуктов IBM Tivoli для обеспечения безопасности КИС

- IBM Tivoli Security Operations Manager;
- IBM Tivoli Management Framework и др.

IBM Tivoli Identity Manager представляет собой автоматизированное, защищенное и основанное на политиках решение по управлению пользователями. IBM Tivoli Identity Manager предоставляет:

- интуитивно понятный веб-интерфейс администрирования;
- сложную модель администрирования на основе ролей, которая позволяет делегировать административные полномочия;
- веб-интерфейсы самообслуживания и запросов/ответов;
- встроенный механизм документооборота для автоматической отправки пользовательских запросов на утверждение, а утвержденных запросов — на выполнение;

- встроенный механизм автоматизации выполнения административных запросов;
- набор инструментов для управления приложениями.

Используя интерфейс самообслуживания и интерфейс делегирования администраторских полномочий на основе ролей, администратор может объединять пользователей в группы в соответствии с потребностями бизнеса и при необходимости делегировать определенные функции управления (право добавлять, удалять, изменять, просматривать учетные записи пользователей и сбрасывать пароли) другим организациям и подразделениям. Помощники администраторов, облеченные теми или иными полномочиями, благодаря политикам на основе задач могут видеть только то, к чему им предоставлен доступ.

IBM Tivoli Access Manager for e-business — это универсальное решение для управления доступом на основе политик, предназначенное для электронного бизнеса и корпоративных приложений. Tivoli Access Manager for e-business позволяет организациям управлять как проводным, так и беспроводным доступом к приложениям и данным, обеспечивая возможность единого входа в систему (SSO) для авторизованных пользователей. Это решение обеспечивает комплексную безопасность, в том числе персональную веб-регистрацию, распределенное веб-администрирование и безопасность с учетом политик. Может интегрироваться с приложениями электронного бизнеса для создания безопасной настраиваемой рабочей среды для авторизованных пользователей. Обеспечивает эффективную организацию аудита доступа пользователей к информационным ресурсам и формирование отчетов аудита.

IBM Tivoli Access Manager for Enterprise Single Sign-On (TAM E-SSO) обеспечивает строгую одношаговую аутентификацию, позволяющую пользователям использовать один пароль для входа во все необходимые им приложения, включая корпоративные приложения и приложения в Интернете. TAM E-SSO позволяет осуществлять регистрацию с помощью одного пароля практически для любого Windows-, веб- или разработанного внутри компании приложения. TAM E-SSO использует приложение-агент, устанавливаемое на ПК пользователя, которое отвечает на запросы приложения (на ввод идентификационных данных пользователя) от имени пользователя. Агент автоматически предоставляет приложению все данные, необходимые для аутентификации пользователя, включая имя пользователя, пароль или другие данные, требуемые приложением. TAM E-SSO повышает безопасность за счет широкого выбора факторов строгой аутентификации и обеспечивает ведение отчетности о соответствии требованиям всех приложений в пределах предприятия.

Программные продукты IBM Tivoli Security Operations Manager и IBM Tivoli Compliance Insight Manager позволяют централизованно управлять и реагировать на различные угрозы и попытки вторжения, направленные на информационные ресурсы предприятия. Эти продукты обладают следующими возможностями.

IBM Tivoli Security Operations Manager (TSOM) — это платформа для повышения эффективности и прозрачности действий по обеспече-

нию безопасности и управлению информационными рисками. TSOM обеспечивает оперативный мониторинг событий безопасности и предназначен в основном для снижения рисков и угроз, исходящих от внешних нарушителей и технологий. TSOM представляет собой набор программных модулей для построения системы сбора и корреляции сообщений от различных устройств и программ обеспечения информационной безопасности. TSOM предназначен для служб эксплуатации систем информационной безопасности; он позволяет автоматизировать часто повторяющиеся и трудоемкие операции, применяемые специалистами для своевременного обнаружения угроз.

IBM Tivoli Compliance Insight Manager (TCIM) осуществляет контроль преимущественно за внутренними угрозами, исходящими от пользователей, в том числе с высокими полномочиями доступа (администраторов сетей, баз данных, ОС, приложений). TCIM обеспечивает корреляцию событий безопасности от различных источников: операционных систем, СУБД, приложений, сетевых устройств, средств безопасности, мэйнфреймов, приведение полученных больших объемов информации о событиях безопасности к удобному для восприятию виду (кто, что, где, когда, откуда, куда), возможности расследования инцидентов, контроль за действиями внутренних пользователей, сторонних консультантов, контроль соответствия нормативным требованиям (включая ISO 27001, ISO 17799 и др.).

IBM Tivoli Management Framework создает вычислительную и коммуникационную основу для функционирования всех модулей Tivoli, обеспечивая тесную интеграцию компонентов Tivoli, стандартные интерфейсы, средства для расширения функциональности, кросс-платформенность и возможность включения собственных приложений в единую систему управления. Содержащийся в Tivoli Framework управляющий агент обслуживает все остальные модули Tivoli. Этот агент устанавливается на компьютер один раз, так что при добавлении новой функциональности необходимо установить только серверную часть соответствующего модуля. После этого новые функции управления будут доступны на всех компьютерах с управляющим агентом Tivoli.

Программные средства превентивной защиты подразделения IBM ISS

Подразделение IBM Internet Security Systems (IBM ISS) предлагает средства превентивной защиты для обеспечения безопасности ИТ-инфраструктуры предприятия. Эти средства превентивной защиты тесно интегрированы с существующими бизнес-процессами предприятия и предназначены для комплексного укрепления всей инфраструктуры — от шлюза до ядра сети, от центра до самых удаленных точек.

Ведущую роль среди средств превентивной защиты играет семейство продуктов IBM Proventia. Это мощная интегрированная платформа для защиты сети, рабочих станций и серверов, в которую включены

средства антивирусной защиты, брандмауэр, виртуальные частные сети (VPN), средства обнаружения и предотвращения сетевых атак, средства обеспечения безопасности приложений, средства защиты от спама, средства фильтрации контента и единый центр управления этими средствами защиты IBM Proventia Management SiteProtector.

Система управления безопасностью IBM Proventia Management SiteProtector

Система централизованного управления IBM Proventia Management SiteProtector выпускается в виде программного комплекса и как программно-аппаратное устройство. Система управления SiteProtector решает следующие основные задачи.

Управление средствами защиты. SiteProtector позволяет управлять всем спектром продуктов IBM ISS. Помимо этого имеется возможность управления средствами защиты информации третьих фирм, включая межсетевые экраны, средства построения VPN и т. д.

Сбор и отображение событий в реальном режиме времени. Каждое устройство семейства Proventia или агент системы защиты сообщает системе SiteProtector обо всех детектируемых событиях. Кроме того, могут быть подключены системы защиты третьих фирм. По каждому из зафиксированных событий предоставляется подробная информация.

Фильтрация событий на консоли управления. В системе SiteProtector используются фильтры событий для сокращения массы данных, отображаемых на консоли. На этапе анализа событий используется модуль корреляции данных Security Fusion. Предопределенные фильтры позволяют быстро выяснить следующие данные:

- кто атакует выбранные ресурсы;
- какие ресурсы являются источниками атак;
- какие узлы уязвимы;
- какие узлы атакуют;
- какие уязвимости на выбранных ресурсах;
- какие атаки нанесли ущерб.

Автоматическое обновление компонентов средств защиты (X-Press Update). В системе SiteProtector реализован механизм X-Press Update, который позволяет автоматически и своевременно получать обновления базы данных уязвимостей и атак из специального хранилища по каналу, защищенному от несанкционированного доступа.

Система генерации отчетов. SiteProtector включает в себя множество предустановленных категорий отчетов. Отчеты могут отображаться как в графическом, так и в текстовом виде.

Основные достоинства:

- *система управления на аппаратной платформе* — возможность приобретения устройства с предустановленным программным обеспечением (SiteProtector Management Appliance SP1001);

- *работа с ролями и правами доступа.* В SiteProtector реализованы механизмы объединения пользователей в группы и составления модели полномочий пользователей. Благодаря модели полномочий механизм создания и сопровождения групп пользователей приобретает большую гибкость и эластичность;
- *поддержка отказоустойчивой конфигурации.* Модуль SecureSync реализует механизм отказоустойчивой конфигурации для системы управления SiteProtector.

Вопросы для самоконтроля

1. Назовите основные задачи системы управления информационной безопасностью КИС.
2. Как осуществляется управление учетными записями и правами доступа к рабочим станциям, серверам и другим активным устройствам КИС?
3. В чем суть концепции глобального управления безопасностью GSM?
4. Объясните понятия глобальной и локальной политик безопасности.
5. Опишите функционирование системы управления информационной безопасностью GSM.
6. Как осуществляется защита ресурсов в системе управления информационной безопасностью GSM?
7. Как осуществляется управление средствами информационной безопасности масштаба предприятия в системе GSM?
8. Опишите централизованное управление безопасностью, реализованное в продуктах «ЗАСТАВА».
9. Опишите возможности системы управления Cisco Security Manager и программно-аппаратного комплекса управления Cisco MARS.
10. Какие функции реализуют продукты IBM Tivoli для обеспечения информационной безопасности КИС?
11. Назовите основные продукты IBM Tivoli и опишите их возможности.
12. Какие задачи решает система управления безопасностью IBM Proventia Management SiteProtector?

Глава 16
СТАНДАРТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Проблемой информационной компьютерной безопасности начали заниматься с того самого момента, когда компьютер стал обрабатывать данные, ценность которых высока для пользователя. В последние годы в связи с ростом спроса на электронные услуги и развитием компьютерных систем и сетей ситуация в сфере информационной безопасности серьезно обострилась, а вопрос стандартизации подходов к ее решению стал особенно актуальным как для разработчиков, так и для пользователей ИТ-средств.

16.1. Роль стандартов информационной безопасности

Главная задача стандартов информационной безопасности — создать основу для взаимодействия между производителями, потребителями и экспертами по квалификации продуктов информационных технологий. Каждая из этих групп имеет свои интересы и свои взгляды на проблему информационной безопасности.

Потребители заинтересованы в методике, позволяющей обоснованно выбрать продукт, отвечающий их нуждам и решающий их проблемы, для чего им необходима шкала оценки безопасности. Потребители также нуждаются в инструменте, с помощью которого они могли бы формулировать свои требования производителям. При этом потребителей интересуют исключительно характеристики и свойства конечного продукта, а не методы и средства их достижения. К сожалению, многие потребители не понимают, что требования безопасности обязательно противоречат функциональным требованиям (удобству работы, быстродействию и т. д.), накладывают ограничения на совместимость и, как правило, вынуждают отказаться от широко распространенных и поэтому незащищенных прикладных программных средств.

Производители нуждаются в стандартах как средстве сравнения возможностей своих продуктов и в применении процедуры сертификации как механизма объективной оценки их свойств, а также в стандартизации определенного набора требований безопасности, который мог бы

ограничить фантазию заказчика конкретного продукта и заставить его выбирать требования из этого набора. С точки зрения производителя, требования должны быть максимально конкретными и регламентировать необходимость применения тех или иных средств, механизмов, алгоритмов и т. д. Кроме того, требования не должны противоречить существующим парадигмам обработки информации, архитектуре вычислительных систем и технологиям создания информационных продуктов. Этот подход также нельзя принять в качестве доминирующего, так как он не учитывает нужд пользователей и пытается подогнать требования защиты под существующие системы и технологии.

Эксперты по квалификации и *специалисты по сертификации* рассматривают стандарты как инструмент, позволяющий им оценить уровень безопасности, обеспечиваемый продуктами информационных технологий, и предоставить потребителям возможность сделать обоснованный выбор. Эксперты по квалификации находятся в двойственном положении: с одной стороны, они, как и производители, заинтересованы в четких и простых критериях, над которыми не надо ломать голову, как их применить к конкретному продукту, а с другой стороны, они должны дать обоснованный ответ пользователям, удовлетворяет продукт их нужды или нет. Таким образом, перед стандартами информационной безопасности стоит непростая задача — примирить три разные точки зрения и создать эффективный механизм взаимодействия всех сторон. Причем ущемление потребностей хотя бы одной из них приведет к невозможности взаимопонимания и взаимодействия и, следовательно, не позволит решить общую задачу — создание защищенной системы обработки информации.

Необходимость в таких стандартах была осознана достаточно давно, и в этом направлении достигнут существенный прогресс, закрепленный в документах разработки 1990-х годов. Первым и наиболее известным документом была Оранжевая книга (по цвету обложки) «Критерии безопасности компьютерных систем» Министерства обороны США. В этом документе определены четыре уровня безопасности — D, C, B и A. По мере перехода от уровня D до A к надежности систем предъявляются все более жесткие требования. Уровни C и B подразделяются на классы (C1, C2, B1, B2, B3). Чтобы система в результате процедуры сертификации могла быть отнесена к некоторому классу, ее защита должна удовлетворять оговоренным требованиям. К другим важным стандартам информационной безопасности этого поколения относятся руководящие документы Гостехкомиссии России, Европейские критерии безопасности информационных технологий, Федеральные критерии безопасности информационных технологий США, Канадские критерии безопасности компьютерных систем [7].

В последнее время в разных странах появилось новое поколение стандартов в области защиты информации, посвященных практическим вопросам управления информационной безопасностью компании. Это прежде всего международные стандарты управления информационной безопасностью ISO 15408, ISO 17799 и некоторые другие. Пред-

ставляется целесообразным проанализировать наиболее важные из этих документов, сопоставить содержащиеся в них требования и критерии, а также оценить эффективность их практического применения.

16.2. Международные стандарты информационной безопасности

В соответствии с международными и национальными стандартами обеспечение информационной безопасности в любой компании предполагает следующее:

- определение целей обеспечения информационной безопасности компьютерных систем;
- создание эффективной системы управления информационной безопасностью;
- расчет совокупности детализированных качественных и количественных показателей для оценки соответствия информационной безопасности поставленным целям;
- применение инструментария обеспечения информационной безопасности и оценки ее текущего состояния;
- использование методик управления безопасностью, позволяющих объективно оценить защищенность информационных активов и управлять информационной безопасностью компании.

Рассмотрим наиболее известные международные стандарты в области защиты информации, которые могут быть использованы в отечественных условиях [6, 7].

16.2.1. Стандарты ISO/IEC 17799:2002 (BS 7799:2000)

В настоящее время международный стандарт ISO/IEC 17799:2000 (BS 7799-1:2000) «Управление информационной безопасностью — Информационные технологии» (Information technology — Information security management) является одним из наиболее известных в области защиты информации. Данный стандарт был разработан на основе первой части британского стандарта BS 7799-1:1995 «Практические рекомендации по управлению информационной безопасностью» (Information security management — Part 1: Code of practice for information security management) и относится к новому поколению стандартов информационной безопасности компьютерных информационных систем.

Текущая версия стандарта ISO/IEC 17799:2000 (BS 7799-1:2000) рассматривает следующие актуальные вопросы обеспечения информационной безопасности организаций и предприятий:

- необходимость обеспечения информационной безопасности;
- основные понятия и определения информационной безопасности;
- политика информационной безопасности компании;

- организация информационной безопасности на предприятии;
- классификация и управление корпоративными нформационными ресурсами;
- кадровый менеджмент и информационная безопасность;
- физическая безопасность;
- администрирование безопасности корпоративных информационных систем;
- управление доступом;
- требования по безопасности к корпоративным информационным системам в ходе их разработки, эксплуатации и сопровождения;
- управление бизнес-процессами компании с точки зрения информационной безопасности;
- внутренний аудит информационной безопасности компании.

Вторая часть стандарта BS 7799-2:2000 «Спецификации систем управления информационной безопасностью» (Information security management — Part 2: Specification for information security management systems) определяет возможные функциональные спецификации корпоративных систем управления информационной безопасностью с точки зрения их проверки на соответствие требованиям первой части данного стандарта. В соответствии с положениями этого стандарта также регламентируется процедура аудита информационных корпоративных систем.

Дополнительные рекомендации для управления информационной безопасностью содержат руководства Британского института стандартов (British Standards Institution — BSI), изданные в период 1995—2003 гг. в виде следующей серии:

- «Введение в проблему управления информационной безопасности» (Information security managment: an introduction);
- «Возможности сертификации на требования стандарта BS 7799» (Preparing for BS 7799 sertification);
- «Руководство BS 7799 по оценке и управлению рисками» (Guide to BS 7799 risk assessment and risk management);
- «Руководство для проведения аудита на требования стандарта» (BS 7799 Guide to BS 7799 auditing);
- «Практические рекомендации по управлению безопасностью информационных технологий» (Code of practice for IT management).

В 2002 г. международный стандарт ISO 17799 (BS 7799) был пересмотрен и существенно дополнен. В новом варианте этого стандарта большое внимание уделено вопросам повышения культуры защиты информации в различных международных компаниях, в том числе вопросам обучения и изначальной интеграции процедур и механизмов оценки и управления информационной безопасности в информационные технологии корпоративных систем. По мнению специалистов, обновление международного стандарта ISO 17799 (BS 7799) позволит не только повысить культуру защиты информационных активов компании, но и скоординировать действия различных ведущих государственных и коммерческих структур в области защиты информации.

16.2.2. Германский стандарт BSI

В отличие от ISO 17799 германское «Руководство по защите информационных технологий для базового уровня защищенности» посвящено детальному рассмотрению частных вопросов управления информационной безопасностью компании.

В германском стандарте BSI представлены:

- общая методика управления информационной безопасностью (организация менеджмента в области ИБ, методология использования руководства);
- описания компонентов современных информационных технологий;
- описания основных компонентов организации режима информационной безопасности (организационный и технический уровни защиты данных, планирование действий в чрезвычайных ситуациях, поддержка непрерывности бизнеса);
- характеристики объектов информатизации (здания, помещения, кабельные сети, контролируемые зоны);
- характеристики основных информационных активов компании (в том числе аппаратного и программного обеспечения, например рабочих станций и серверов под управлением операционных систем семейства DOS, Windows и UNIX);
- характеристики компьютерных сетей на основе различных сетевых технологий, например сетей Novell NetWare, UNIX и Windows;
- характеристики активного и пассивного телекоммуникационного оборудования ведущих поставщиков, например Cisco Systems;
- подробные каталоги угроз безопасности и мер контроля (более 600 наименований в каждом каталоге).

Вопросы защиты приведенных информационных активов компании рассматриваются по определенному сценарию: общее описание информационного актива компании — возможные угрозы и уязвимости безопасности — возможные меры и средства контроля и защиты.

16.2.3. Международный стандарт ISO 15408 «Общие критерии безопасности информационных технологий»

Одним из главных результатов стандартизации в сфере систематизации требований и характеристик защищенных информационных комплексов стала система международных и национальных стандартов безопасности информации, которая насчитывает более сотни различных документов. Важное место в этой системе стандартов занимает стандарт ISO 15408, известный как «Общие критерии» (Common Criteria).

В 1990 г. Международная организация по стандартизации (ISO) приступила к разработке международного стандарта по критериям

оценки безопасности информационных технологий для общего использования под названием «Общие критерии оценки безопасности информационных технологий».

В разработке «Общих критериев» (ОК) участвовали Национальный институт стандартов и технологии и Агентство национальной безопасности (США), Учреждение безопасности коммуникаций (Канада), Агентство информационной безопасности (Германия), Агентство национальной безопасности коммуникаций (Голландия), органы исполнения Программы безопасности и сертификации ИТ (Англия), Центр обеспечения безопасности систем (Франция), которые опирались на свой солидный опыт.

«Общие критерии» обобщили содержание и опыт использования Оранжевой книги, развили европейские и канадские критерии и воплотили в реальные структуры концепцию типовых профилей защиты федеральных критериев США.

За десятилетие разработки «Общие критерии» неоднократно редактировались лучшими специалистами мира. В результате был подготовлен международный стандарт ISO/IEC 15408.

Первые две версии «Общих критериев» были опубликованы соответственно в январе и мае 1998 г. Версия 2.1 этого стандарта утверждена 8 июня 1999 г. Международной организацией по стандартизации в качестве международного стандарта информационной безопасности ISO/IEC 15408 под названием «Общие критерии оценки безопасности информационных технологий».

В ОК проведена классификация широкого набора требований безопасности ИТ, определены структуры их группирования и принципы использования. Главные достоинства ОК — полнота требований безопасности и их систематизация, гибкость в применении и открытость для последующего развития.

«Общие критерии» адаптированы к потребностям взаимного признания результатов оценки безопасности ИТ в мировом масштабе и предназначены для использования в качестве основы для такой оценки. Они позволяют сравнить результаты независимых оценок информационной безопасности и допустимых рисков на основе множества общих требований к функциям безопасности средств и систем ИТ, а также гарантий, применяемых к ним в процессе тестирования.

Основываясь на общем перечне (наборе) требований, в процессе выработки оценки уровня защиты устанавливается уровень доверия. Результаты оценок защиты позволяют определить для компании достаточность защиты корпоративной информационной системы.

Ведущие мировые производители оборудования ИТ основательно подготовились к этому моменту и сразу стали поставлять заказчикам средства, полностью отвечающие требованиям ОК.

Принятый базовый стандарт информационной безопасности ISO 15408, безусловно, очень важен для российских разработчиков.

«Общие критерии» разрабатывались в расчете на то, чтобы удовлетворить запросы трех групп специалистов, в равной степени являющих-

ся пользователями этого документа: производителей и потребителей продуктов информационных технологий, а также экспертов по оценке уровня их безопасности. «Общие критерии» обеспечивают нормативную поддержку процесса выбора ИТ-продукта, к которому предъявляются требования функционирования в условиях действия определенных угроз, служат руководящим материалом для разработчиков таких систем, а также регламентируют технологию их создания и процедуру оценки обеспечиваемого уровня безопасности.

«Общие критерии», во-первых, рассматривают информационную безопасность как совокупность конфиденциальности и целостности информации, обрабатываемой ИТ-продуктом, а также доступности ресурсов ВС и, во-вторых, ставят перед средствами защиты задачу противодействия угрозам, актуальным для среды эксплуатации этого продукта и реализации политики безопасности, принятой в этой среде эксплуатации. Поэтому в концепцию «Общих критериев» входят все аспекты процесса проектирования, производства и эксплуатации ИТ-продуктов, предназначенных для работы в условиях действия определенных угроз безопасности.

Потребители ИТ-продуктов озабочены наличием угроз безопасности, приводящих к определенным рискам для обрабатываемой информации. Для противодействия этим угрозам ИТ-продукты должны включать в свой состав средства защиты, противодействующие этим угрозам и направленные на устранение уязвимостей, однако ошибки в средствах защиты, в свою очередь, могут приводить к появлению новых уязвимостей. Сертификация средств защиты позволяет подтвердить их адекватность угрозам и рискам.

«Общие критерии» регламентируют все стадии разработки, квалификационного анализа и эксплуатации ИТ-продуктов. «Общие критерии» предлагают концепцию процесса разработки и квалификационного анализа ИТ-продуктов, требующую от потребителей и производителей большой работы по составлению и оформлению довольно объемных и подробных нормативных документов.

Требования «Общих критериев» являются практически всеобъемлющей энциклопедией информационной безопасности, поэтому их можно использовать в качестве справочника по безопасности информационных технологий.

Стандарт ISO 15408 поднял стандартизацию информационных технологий на межгосударственный уровень. Возникла реальная перспектива создания единого безопасного информационного пространства, в котором сертификация безопасности систем обработки информации будет осуществляться на глобальном уровне, что предоставит возможности для интеграции национальных информационных систем, а это, в свою очередь, откроет новые сферы применения информационных технологий.

Некоторые особенности стандарта ISO 15408 приводятся в разделе 12.3, где рассматривается стандарт ГОСТ Р ИСО/МЭК 15408, являющийся аналогом стандарта ISO 15408.

16.2.4. Стандарты для беспроводных сетей

Стандарт IEEE 802.11

В 1990 г. Комитет IEEE 802 сформировал рабочую группу 802.11 для разработки стандарта для беспроводных локальных сетей WLAN (Wireless Local Area Network). Работы по созданию стандарта были завершены через 7 лет. В 1997 г. была ратифицирована первая спецификация беспроводного стандарта IEEE 802.11, обеспечивающего передачу данных с гарантированной скоростью 1 Мбит/с (в некоторых случаях до 2 Мбит/с) в полосе частот 2,4 ГГц. Эта полоса частот доступна для нелицензионного использования в большинстве стран мира.

Стандарт IEEE 802.11 является базовым стандартом и определяет протоколы, необходимые для организации беспроводных локальных сетей. Основные из них — протокол управления доступом к среде MAC (Medium Accsess Control — нижний подуровень канального уровня) и протокол PHY передачи сигналов в физической среде. В качестве физической среды допускается использование радиоволн и инфракрасного излучения.

В основу стандарта IEEE 802.11 положена сотовая архитектура, причем сеть может состоять как из одной, так и из нескольких ячеек. Каждая сота управляется базовой станцией, называемой *точкой доступа AP (Access Point)*, которая вместе с находящимися в пределах радиуса ее действия рабочими станциями пользователей образует *базовую зону обслуживания BSS (Basic Service Set)*. Точки доступа многосотовой сети взаимодействуют между собой через *распределительную систему DS (Distribution System)*, представляющую собой эквивалент магистрального сегмента кабельных ЛС. Вся инфраструктура, включающая точки доступа и распределительную систему, образует *расширенную зону обслуживания ESS (Extended Service Set)*. Стандартом предусмотрен также односотовый вариант беспроводной сети, который может быть реализован и без точки доступа, при этом часть ее функций выполняется непосредственно рабочими станциями.

Для обеспечения перехода мобильных рабочих станций из зоны действия одной точки доступа к другой в многосотовых системах предусмотрены специальные процедуры сканирования (активного и пассивного прослушивания эфира) и присоединения (Association), однако строгих спецификаций по реализации роуминга стандарт 802.11 не предусматривает.

Для защиты WLAN стандартом IEEE 802.11 предусмотрен алгоритм WEP (Wired Equivalent Privacy). Он включает средства противодействия несанкционированному доступу к сети, а также шифрование для предотвращения перехвата информации.

Однако заложенная в первую спецификацию стандарта IEEE 802.11 скорость передачи данных в беспроводной сети уже не удовлетворяла потребностям пользователей. Алгоритм WEP страдал рядом существен-

ных недостатков: отсутствие управления ключом, использование общего статического ключа, малые разрядности ключа и вектора инициализации, сложности использования алгоритма RC4.

Чтобы сделать технологию Wireless LAN недорогой, популярной и удовлетворяющей жестким требованиям бизнес-приложений, разработчики были вынуждены создать семейство новых спецификаций стандарта IEEE 802.11 a, b, ..., i. Стандарты этого семейства, по сути, являются беспроводными расширениями протокола Ethernet, что обеспечивает хорошее взаимодействие с проводными сетями Ethernet.

Стандарт IEEE 802.11b применяется наиболее широко из всех стандартов 802.11, поэтому мы с него и начнем. Высокоскоростной стандарт 802.11b был ратифицирован IEEE в сентябре 1999 г. как развитие базового стандарта 802.11; в стандарте 802.11b используется полоса частот 2,4 ГГц, скорость передачи достигает 11 Мбит/с (подобно Ethernet). Благодаря ориентации на освоенный диапазон 2,4 ГГц стандарт 802.11b завоевал большую популярность у производителей оборудования. В качестве базовой радиотехнологии в нем используется метод распределенного спектра с прямой последовательностью DSSS (Direct Sequence Spread Spectrum), который отличается высокой устойчивостью к искажению данных помехами, в том числе преднамеренными. Этот стандарт получил широкое распространение, и беспроводные LAN стали привлекательным решением с технической и финансовой точки зрения.

Для простоты запоминания в качестве общего имени для стандартов 802.11b и 802.11a, а также всех последующих, относящихся к беспроводным локальным сетям (WLAN), был введен термин *Wi-Fi (Wireless Fidelity)*. Этот термин введен Ассоциацией беспроводной совместимости с Ethernet WECA (Wireless Ethernet Compatibility Aliance). Если устройство помечено этим знаком, оно протестировано на совместимость с другими устройствами 802.11.

Стандарт IEEE 802.11a предназначен для работы в частотном диапазоне 5 ГГц. Скорость передачи данных до 54 Мбит/с, т. е. примерно в пять раз быстрее сетей 802.11b. Ассоциация WECA называет этот стандарт WiFi5. Это наиболее широкополосный из семейства стандартов 802.11. Определены три обязательные скорости — 6, 12 и 24 Мбит/с — и пять необязательных — 9, 18, 36, 48 и 54 Мбит/с. В качестве метода модуляции сигнала принято ортогональное частотное мультиплексирование OFDM (Orthogonal Frequency Division Multiplexing). Его отличие от метода DSSS заключается в том, что OFDM предполагает параллельную передачу полезного сигнала одновременно по нескольким частотам диапазона, в то время как технологии расширения спектра DSSS передают сигналы последовательно. В результате повышается пропускная способность канала и качество сигнала. К недостаткам стандарта 802.11a относятся большая потребляемая мощность радиопередатчиков для частот 5 ГГц, а также меньший радиус действия (около 100 м).

Стандарт IEEE 802.11g представляет собой развитие 802.11b и обратно совместим с 802.11b. Предназначен для обеспечения скоростей

передачи данных до 54 Мбит/с. В числе достоинств 802.11g надо отметить низкую потребляемую мощность, большие расстояния (до 300 м) и высокую проникающую способность сигнала.

Стандарт IEEE 802.11i. В 2004 г. IEEE ратифицировал стандарт обеспечения безопасности в беспроводных сетях IEEE 802.11i. Этот стандарт решил существовавшие проблемы в области аутентификации и протокола шифрования, обеспечив значительно более высокий уровень безопасности. Стандарт 802.11i может применяться в сетях Wi-Fi независимо от используемого стандарта — 802.11a, b или g.

В настоящее время существует два очень похожих стандарта — WPA и 802.11i. Они оба применяют механизм 802.1x для обеспечения надежной аутентификации, оба используют сильные алгоритмы шифрования, оба предназначены для замены протокола WEP.

WPA был разработан в Wi-Fi Alliance как решение, которое можно применить немедленно, не дожидаясь завершения длительной процедуры ратификации 802.11i в IEEE.

Основное отличие двух стандартов заключается в использовании различных механизмов шифрования. В WPA применяется протокол TKIP (Temporal Key Integrity Protocol), который, так же как и WEP, использует шифр RC4, но значительно более безопасным способом. Обеспечение конфиденциальности данных в стандарте IEEE 802.11i основано на использовании алгоритма шифрования AES. Использующий его защитный протокол получил название CCMP (Counter-Mode CBC MAC Protocol). Алгоритм AES обладает высокой криптостойкостью. Длина ключа AES равна 128, 192 или 256 бит, что обеспечивает наиболее надежное шифрование из доступных сейчас.

Стандарт 802.11i предполагает наличие трех участников процесса аутентификации. Это сервер аутентификации AS (Authentication Server), точка доступа AP (Access Point) и рабочая станция STA (Station). В процессе шифрования данных участвуют только AP и STA (AS не используется). Стандарт предусматривает двустороннюю аутентификацию (в отличие от WEP, где аутентифицируется только рабочая станция, но не точка доступа). При этом местами принятия решения о разрешении доступа являются сервер аутентификации AS и рабочая станция STA, а местами исполнения этого решения — точка доступа AP и STA.

Для работы по стандарту 802.11i создается иерархия ключей, включающая мастер-ключ MK (Master Key), парный мастер-ключ PMK (Pairwise Master Key), парный временный ключ PTK (Pairwise Transient Key), а также групповые временные ключи GTK (Group Transient Key), служащие для защиты широковещательного сетевого трафика.

MK — это симметричный ключ, реализующий решение STA и AS о взаимной аутентификации. Для каждой сессии создается новый MK.

PMK — обновляемый симметричный ключ, владение которым означает разрешение (авторизацию) на доступ к среде передачи данных в течение данной сессии. PMK создается на основе MK. Для каждой пары STA и AP в каждой сессии создается новый PMK.

PTK — это коллекция операционных ключей, которые используются для привязки PMK к данным STA и AP, для распространения GTK и шифрования данных.

Процесс аутентификации и доставки ключей определяется стандартом 802.1x. Он предоставляет возможность использовать в беспроводных сетях такие традиционные серверы аутентификации, как RADIUS. Стандарт 802.11i не определяет тип сервера аутентификации, но использование RADIUS для этой цели является стандартным решением.

Транспортом для сообщений 802.1x служит протокол EAP (Extensible Authentication Protocol). EAP позволяет легко добавлять новые методы аутентификации. Точке доступа не требуется знать об используемом методе аутентификации, поэтому изменение метода никак не затрагивает точку доступа.

Наиболее популярные методы EAP — это LEAP, PEAP, TTLS и FAST. Каждый из методов имеет свои сильные и слабые стороны, условия применения, по-разному поддерживается производителями оборудования и программного обеспечения.

Можно выделить пять фаз работы 802.11i.

Первая фаза — обнаружение. В этой фазе рабочая станция STA находит точку доступа AP, с которой может установить связь, и получает от нее используемые в данной сети параметры безопасности. Таким образом, STA узнает идентификатор сети SSID и методы аутентификации, доступные в данной сети. Затем STA выбирает метод аутентификации, и между STA и AP устанавливается соединение. После этого STA и AP готовы к началу второй фазы. 802.1x.

Вторая фаза — аутентификация. В этой фазе выполняется взаимная аутентификация STA и сервера AS, создаются MK и PMK. В данной фазе STA и AP блокируют весь трафик, кроме трафика 802.1x.

В *третьей фазе* AS перемещает ключ PMK на AP. Теперь STA и AP владеют действительными ключами PMK.

Четвертая фаза — управление ключами 802.1x. В этой фазе происходит генерация, привязка и верификация ключа PTK.

Пятая фаза — шифрование и передача данных. Для шифрования используется соответствующая часть PTK.

Стандартом 802.11i предусмотрен режим PSK (Pre-Shared Key), который позволяет обойтись без сервера аутентификации AS. При использовании этого режима на STA и на AP вручную вводится Pre-Shared Key, который используется в качестве PMK. Дальше генерация PTK происходит описанным выше порядком. Режим PSK может использоваться в небольших сетях, где нецелесообразно устанавливать сервер AS.

16.2.5. Стандарты информационной безопасности для Интернета

В последнее время в мире бурно развивается электронная коммерция посредством сети Интернет. Развитие электронной коммерции в основном определяется прогрессом в области безопасности информации. При

этом базовыми задачами являются обеспечение доступности, конфиденциальности, целостности и юридической значимости информации.

По оценке Комитета ООН по предупреждению преступности и борьбе с ней, компьютерная преступность вышла на уровень одной из международных проблем. Поэтому чрезвычайно важно добиваться эффективного решения проблем обеспечения безопасности коммерческой информации в глобальной сети Интернет и смежных интранет-сетях, которые по своей технической сущности не имеют принципиальных отличий и различаются в основном масштабами и открытостью.

Рассмотрим особенности стандартизации процесса обеспечения безопасности коммерческой информации в сетях с протоколом передачи данных IP/TCP и с акцентом на защиту телекоммуникаций [104].

Обеспечение безопасности информационных технологий особенно актуально для открытых систем коммерческого применения, обрабатывающих информацию ограниченного доступа, не содержащую государственную тайну. Под открытыми системами понимают совокупности всевозможного вычислительного и телекоммуникационного оборудования разного производства, совместное функционирование которого обеспечивается соответствием требованиям международных стандартов.

Термин «открытые системы» подразумевает также, что если вычислительная система соответствует стандартам, то она будет открыта для взаимосвязи с любой другой системой, которая соответствует тем же стандартам. Это, в частности, относится и к механизмам криптографической защиты информации или к защите от несанкционированного доступа к информации.

Важная заслуга Интернета состоит в том, что он заставил по-новому взглянуть на такие технологии. Во-первых, Интернет поощряет применение открытых стандартов, доступных для внедрения всем, кто проявит к ним интерес. Во-вторых, он представляет собой крупнейшую в мире и, вероятно, единственную сеть, к которой подключается такое множество разных компьютеров. И наконец, Интернет становится общепринятым средством представления быстро меняющейся новой продукции и технологий на мировом рынке.

В Интернете уже давно существует целый ряд комитетов, в основном из организаций-добровольцев, которые осторожно проводят предлагаемые технологии через процесс стандартизации. Эти комитеты, составляющие основную часть Рабочей группы инженеров Интернета IETF (Internet Engineering Task Force), провели стандартизацию нескольких важных протоколов, ускоряя их внедрение в Интернете. Непосредственными результатами усилий IETF являются такие протоколы, как семейство TCP/IP для передачи данных, SMTP и POP для электронной почты, а так же SNMP для управления сетью.

В Интернете популярны протоколы безопасной передачи данных, а именно SSL, SET, IPSec. Перечисленные протоколы появились в Интернете сравнительно недавно в ответ на необходимость защиты ценной информации и сразу стали стандартами де-факто.

Протокол SSL

Протокол SSL (Secure Socket Layer) является сейчас популярным сетевым протоколом с шифрованием данных для безопасной передачи по сети. Он позволяет устанавливать защищенное соединение, производить контроль целостности данных и решать различные сопутствующие задачи. Протокол SSL обеспечивает защиту данных между сервисными протоколами (такими как HTTP, FTP и др.) и транспортными протоколами (TCP/IP) с помощью современной криптографии.

Протокол IPSec

Спецификация IPSec входит в стандарт IP v.6 и является дополнительной по отношению к текущей версии протоколов TCP/IP. Она разработана Рабочей группой IP Security IETF. В настоящее время IPSec включает три алгоритмо-независимые базовые спецификации, представляющие соответствующие RFC-стандарты. Протокол IPSec обеспечивает стандартный способ шифрования трафика на сетевом (третьем) уровне IP и защищает информацию на основе сквозного шифрования, независимо от работающего приложения, при этом шифруется каждый пакет данных, проходящий по каналу. Это позволяет организациям создавать в Интернете виртуальные частные сети.

Протокол SET

Протокол SET (Security Electronics Transaction) — перспективный стандарт безопасных электронных транзакций в сети Интернет, предназначенный для организации электронной торговли через Интернет. Протокол SET основан на использовании цифровых сертификатов по стандарту X.509.

Протокол выполнения защищенных транзакций SET является стандартом, разработанным компаниями MasterCard и Visa при значительном участии IBM, GlobeSet и других партнеров. Он позволяет покупателям приобретать товары через Интернет, используя защищенный механизм выполнения платежей.

SET является открытым стандартным многосторонним протоколом для проведения безопасных платежей с использованием пластиковых карточек в Интернете. SET обеспечивает кросс-аутентификацию счета держателя карты, продавца и банка продавца для проверки готовности оплаты, а также целостность и секретность сообщения, шифрование ценных и уязвимых данных. Поэтому SET более правильно было бы назвать стандартной технологией или системой протоколов выполнения безопасных платежей с использованием пластиковых карт через Интернет. SET позволяет потребителям и продавцам подтвердить подлинность всех участников сделки, происходящей в Интернете, с помощью криптографии, в том числе применяя цифровые сертификаты.

Объем потенциальных продаж в области электронной коммерции ограничивается достижением необходимого уровня безопасности информации, который обеспечивают вместе покупатели, продавцы и финансовые институты, обеспокоенные вопросами безопасности в Интернете. Как упоминалось ранее, базовыми задачами защиты информации являются обеспечение ее доступности, конфиденциальности, целостности и юридической значимости. SET, в отличие от других протоколов, позволяет решать указанные задачи защиты информации в целом.

SET, в частности, обеспечивает следующие специальные требования защиты операций электронной коммерции:

- секретность данных оплаты и конфиденциальность информации заказа, переданной наряду с данными об оплате;
- сохранение целостности данных платежей. Целостность информации платежей обеспечивается с помощью цифровой подписи;
- специальную криптографию с открытым ключом для проведения аутентификации;
- аутентификацию держателя по кредитной карточке. Она обеспечивается применением цифровой подписи и сертификатов держателя карт;
- аутентификацию продавца и его возможности принимать платежи по пластиковым карточкам с применением цифровой подписи и сертификатов продавца;
- аутентификацию того, что банк продавца является действующей организацией, которая может принимать платежи по пластиковым карточкам через связь с процессинговой карточной системой. Аутентификация банка продавца обеспечивается использованием цифровой подписи и сертификатов банка продавца;
- готовность оплаты транзакций в результате аутентификации сертификата с открытым ключом для всех сторон;
- безопасность передачи данных посредством преимущественного использования криптографии.

Основное преимущество SET по сравнению с многими существующими системами обеспечения информационной безопасности заключается в использовании цифровых сертификатов (стандарт X509, версия 3), которые ассоциируют держателя карты, продавца и банк продавца с рядом банковских учреждений платежных систем Visa и Mastercard. Кроме того, SET позволяет сохранить существующие отношения между банком, держателями карт и продавцами и интегрируется с существующими системами.

Инфраструктура управления открытыми ключами PKI

Инфраструктура управления открытыми ключами PKI (Public Key Infrastructure) предназначена для защищенного управления криптографическими ключами электронного документооборота, основанного на применении криптографии с открытыми ключами. Эта инфраструктура

подразумевает использование цифровых сертификатов, удовлетворяющих рекомендациям международного стандарта X.509 и развернутой сети центров сертификации, обеспечивающих выдачу и сопровождение цифровых сертификатов для всех участников электронного обмена документами (см. главу 4).

16.3. Отечественные стандарты безопасности информационных технологий

Исторически сложилось, что в России проблемы безопасности ИТ изучались и своевременно решались в основном в сфере охраны государственной тайны. Аналогичные задачи коммерческого сектора экономики долгое время не находили соответствующих решений.

Информация, содержащаяся в системах или продуктах ИТ, является критическим ресурсом, позволяющим организациям успешно решать свои задачи. Кроме того, частные лица вправе ожидать, что их персональная информация, будучи размещенной в продуктах или системах ИТ, останется приватной, доступной им по мере необходимости и не сможет быть подвергнута несанкционированной модификации.

При выполнении продуктами или системами ИТ их функций следует осуществлять надлежащий контроль информации, что обеспечило бы ее защиту от опасностей нежелательного или неоправданного распространения, изменения или потери. Понятие «безопасность ИТ» охватывает предотвращение и уменьшение этих и аналогичных опасностей.

Проблема защиты информации в коммерческой автоматизированной системе имеет свои особенности, которые необходимо учитывать, поскольку они оказывают серьезное влияние на информационную безопасность. Перечислим основные особенности:

1. *Приоритет экономических факторов.* Для коммерческой автоматизированной системы важно снизить либо исключить финансовые потери и обеспечить получение прибыли владельцем и пользователями данного инструментария в условиях реальных рисков. Важным условием при этом, в частности, является минимизация типично банковских рисков (например, потерь за счет ошибочных направлений платежей, фальсификации платежных документов и т. п.).

2. *Открытость проектирования*, предусматривающая создание подсистемы защиты информации из средств, широко доступных на рынке и работающих в открытых системах.

3. *Юридическая значимость коммерческой информации*, которую можно определить как свойство безопасной информации, позволяющее обеспечить юридическую силу электронным документам или информационным процессам в соответствии с законодательством Российской Федерации.

В табл. 16.1 указаны нормативные документы по критериям оценки защищенности средств вычислительной техники и автоматизированных систем и документы, регулирующие информационную безопасность (строки 1—10). Здесь же указаны нормативные документы по криптографической защите систем обработки информации и информационных технологий (строки 11—13).

Таблица 16.1. **Российские стандарты, регулирующие ИБ**

№	Стандарт	Наименование
1	ГОСТ Р ИСО/МЭК 15408-1-2002	Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. Госстандарт России
2	ГОСТ Р ИСО/МЭК 15408-2-2002	Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности. Госстандарт России
3	ГОСТ Р ИСО/МЭК 15408-3-2002	Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности. Госстандарт России
4	ГОСТ Р 50739-95	Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования. Госстандарт России
5	ГОСТ Р 50922-96	Защита информации. Основные термины и определения. Госстандарт России
6	ГОСТ Р 51188-98	Защита информации. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство. Госстандарт России
7	ГОСТ Р 51275-99	Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Госстандарт России
8	ГОСТ Р ИСО 7498-1-99	Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 1. Базовая модель. Госстандарт России
9	ГОСТ Р ИСО 7498-2-99	Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации. Госстандарт России

Окончание табл. 16.1

№	Стандарт	Наименование
10	ГОСТ Р 50739-95	Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования
11	ГОСТ 28147-89	Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования
12	ГОСТ Р 34.10-2001	Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи
13	ГОСТ Р 34.11-94	Информационная технология. Криптографическая защита информации. Функция хэширования

Стандарты в структуре информационной безопасности выступают как связующее звено между технической и концептуальной стороной вопроса.

Введение в 1999 г. международного стандарта ISO 15408 в области обеспечения информационной безопасности имело большое значение как для разработчиков компьютерных информационных систем, так и для их пользователей. Стандарт ISO 15408 стал своего рода гарантией качества и надежности сертифицированных по нему программных продуктов. Этот стандарт позволил потребителям лучше ориентироваться при выборе программного обеспечения и приобретать продукты, соответствующие их требованиям безопасности, и, как следствие этого, повысил конкурентоспособность IT-компаний, сертифицирующих свою продукцию в соответствии с ISO 15408.

Стандарт «Критерии оценки безопасности информационных технологий» ГОСТ Р ИСО/МЭК 15408

С января 2004 г. в России действует стандарт «Критерии оценки безопасности информационных технологий» ГОСТ Р ИСО/МЭК 15408, который является аналогом стандарта ISO 15408. Стандарт ГОСТ Р ИСО/МЭК 15408, называемый еще «Общими критериями», является на сегодня самым полным стандартом, определяющим инструменты оценки безопасности информационных систем и порядок их использования.

«Общие критерии» направлены на защиту информации от несанкционированного раскрытия, модификации, полной или частичной потери и применимы к защитным мерам, реализуемым аппаратными, программно-аппаратными и программными средствами.

«Общие критерии» предназначены служить основой при оценке характеристик безопасности продуктов и систем ИТ. Заложенные в

стандарте наборы требований позволяют сравнивать результаты независимых оценок безопасности. На основании этих результатов потребитель может принимать решение о том, достаточно ли безопасны ИТ-продукты или системы для их применения с заданным уровнем риска.

Стандарт ГОСТ Р ИСО/МЭК 15408 состоит из трех частей.

В первой части (ГОСТ Р ИСО/МЭК 15408-1 «Введение и общая модель») устанавливается общий подход к формированию требований безопасности и оценке безопасности, на их основе разрабатываются основные конструкции (профиль защиты и задание по безопасности) представления требований безопасности в интересах потребителей, разработчиков и оценщиков продуктов и систем ИТ. Требования безопасности объекта оценки (ОО) по методологии «Общих критериев» определяются исходя из целей безопасности, которые основываются на анализе назначения ОО и условий среды его использования (угроз, предположений, политики безопасности).

Часть вторая (ГОСТ Р ИСО/МЭК 15408-2 «Функциональные требования безопасности») содержит универсальный каталог функциональных требований безопасности и предусматривает возможность их детализации и расширения по определенным правилам.

Третья часть (ГОСТ Р ИСО/МЭК 15408-3 «Требования доверия к безопасности») включает в себя систематизированный каталог требований доверия, определяющих меры, которые должны быть приняты на всех этапах жизненного цикла продукта или системы ИТ для обеспечения уверенности в том, что они удовлетворяют предъявленным к ним функциональным требованиям. Здесь же содержатся оценочные уровни доверия (ОУД), определяющие шкалу требований, которые позволяют с возрастающей степенью полноты и строгости оценить проектную, тестовую и эксплуатационную документацию, правильность реализации функций безопасности ОО, уязвимости продукта или системы ИТ, стойкость механизмов защиты, и позволяющие сделать заключение об уровне доверия к безопасности объекта оценки.

Обобщая вышесказанное, можно отметить, что каркас безопасности, заложенный частью 1 стандарта ГОСТ Р ИСО/МЭК 15408, заполняется содержимым из классов, семейств и компонентов в части 2, а третья часть определяет, как оценить прочность всего «строения».

Стандарт «Общие критерии безопасности информационных технологий» отражает достижения последних лет в области информационной безопасности. Впервые документ такого уровня содержит разделы, адресованные потребителям, производителям и экспертам по оценке безопасности ИТ-продуктов.

Главные достоинства стандарта ГОСТ Р ИСО/МЭК 15408:

- полнота требований к информационной безопасности;
- гибкость в применении;
- открытость для последующего развития с учетом новейших достижений науки и техники.

Вопросы для самоконтроля

1. Сформулируйте главную задачу стандартов информационной безопасности с позиций производителей и потребителей продуктов информационных технологий, а также специалистов по сертификации этих продуктов.
2. Назовите основные международные стандарты информационной безопасности.
3. Дайте краткую характеристику международного стандарта ISO/IEC 17799:2000 (BS 7799-1:2000).
4. Каковы основные особенности германского стандарта BSI «Руководство по защите информационных технологий для базового уровня защищенности»?
5. Опишите содержание и укажите значение международного стандарта ISO 15408 «Общие критерии безопасности информационных технологий».
6. Перечислите стандарты для беспроводных сетей и дайте их краткую характеристику.
7. Назовите стандарты информационной безопасности для Интернета.
8. Каковы назначение и особенности функционирования протокола SET?
9. Каковы назначение и функциональность протоколов SSL и IPSec? В чем эти протоколы существенно различаются?
10. Каковы назначение и функциональность инфраструктуры управления открытыми ключами PKI?
11. Перечислите российские стандарты безопасности информационных технологий.
12. Каково назначение стандарта ГОСТ Р ИСО/МЭК 15408? Назовите и охарактеризуйте три основные части этого стандарта.

Литература

1. *Абрамов А. В.* VPN-решения для российских компаний // Конфидент. — 2001. — № 1. — С. 62—67.

2. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. — М.: Гостехкомиссия России, 1992.

3. *Александров А.* Как предотвратить вторжение: второй уровень защиты // BYTE. — 2003. — № 9.

4. *Астахов А. М.* Аудит безопасности информационных систем // Конфидент. — 2003. — № 2.

5. *Ахметов К.* Безопасность в Windows XP // Безопасность. — 2001. — № 12.

6. *Галатенко В. А.* Информационная безопасность — грани практического подхода / Конференция «Корпоративные информационные системы». — М., 1999.

7. *Галицкий А. В., Рябко С. Д., Шаньгин В. Ф.* Защита информации в сети — анализ технологий и синтез решений. — М.: ДМК Пресс, 2004.

8. ГОСТ 28147—89. Система обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. — М.: Госстандарт СССР, 1989.

9. ГОСТ Р 34.10—2001. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи. — М.: Госстандарт России, 2001.

10. ГОСТ Р 34.10—94. Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма. — М.: Госстандарт России, 1994.

11. ГОСТ Р 34.11—94. Информационная технология. Криптографическая защита информации. Функция хэширования. — М.: Госстандарт России, 1994.

12. ГОСТ Р 50739—95. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования. — М.: Госстандарт России, 1995.

13. ГОСТ Р 50922—96. Защита информации. Основные термины и определения. — М.: Госстандарт России, 1996.

14. ГОСТ Р 51275—99. Защита информации. Объект информации. Факторы, воздействующие на информацию. Общие положения. — М.: Госстандарт России, 1999.

15. ГОСТ Р 51583—2000. Защита информации. Порядок создания систем в защищенном исполнении. — М.: Госстандарт России, 2000.

16. ГОСТ Р ИСО/МЭК 15408-1—2002. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. — М.: ИПК «Издательство стандартов», 2002.

17. ГОСТ Р ИСО/МЭК 15408-2—2002. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности. — М.: ИПК «Издательство стандартов», 2002.

18. ГОСТ Р ИСО/МЭК 15408-3—2002. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности. — М.: ИПК «Издательство стандартов», 2002.

19. *Давлетханов М.* Концепция одноразовых паролей в системе аутентификации // BYTE. — 2006. — № 7—8.

20. *Девянин П. Н.* Модели безопасности компьютерных систем: учеб. пособие для студентов вузов. — М.: Академия, 2005.

21. *Диффи У.* Первые десять лет криптографии с открытым ключом // ТИИЭР. — 1988. — Т. 76. — № 5. — С. 54—74.

22. *Дишунян В. Л., Шаньгин В. Ф.* Электронная идентификация. Бесконтактные электронные идентификаторы и смарт-карты. — М.: НТ Пресс, 2004.

23. *Елманова Н.* Безопасность в Microsoft Windows Vista // КомпьютерПресс. — 2007. — № 3.

24. Защита информации. Специальные защитные знаки. Классификация и общие требования. — М.: Гостехкомиссия России, 1992.

25. Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей. — М.: Гостехкомиссия России, 1999.

26. *Зегжда Д. П., Ивашко А. М.* Основы безопасности информационных систем. — М.: Горячая линия — Телеком, 2000.

27. *Зима В. М., Молдовян А. А., Молдовян Н. А.* Безопасность глобальных сетевых технологий. — СПб.: БХВ-Петербург, 2001.

28. ИСО/МЭК 10118-1—94. Информационная технология. Методы защиты. Хэш-функции. Часть 1. Общие положения.

29. ИСО/МЭК 10118-2—94. Информационная технология. Методы защиты. Хэш-функции. Часть 2. Хэш-функции с использованием n-битного блочного алгоритма шифрации.

30. ИСО/МЭК 14888-1—98. Информационная технология. Методы защиты. Цифровые подписи с приложением. Часть 1. Общие положения.

31. ИСО/МЭК 14888-2—99. Информационная технология. Методы защиты. Цифровые подписи с приложением. Часть 2. Механизмы на основе подтверждения подлинности.

32. *Касперский Е.* Компьютерные вирусы: что это такое и как с ними бороться. — М.: СК Пресс, 1998.

33. *Конеев И., Беляев А.* Информационная безопасность предприятия. — СПб.: БХВ-Петербург, 2003.

34. *Коннолли Т., Бегг К.* Базы данных. Проектирование, реализация и сопровождение. Теория и практика. 3-е изд.: пер. с англ. — М.: Вильямс, 2003.

35. *Лукацкий А.* Безопасность беспроводных сетей // Технологии и средства связи. — 2005. — № 1.

36. *Лукацкий А.* Предотвращение сетевых атак: технологии и решения // Экспресс Электроника. — 2006.

37. *Максим М., Полино Д.* Безопасность беспроводных сетей: пер. с англ. — М.: ДМК Пресс, 2004.

38. *Мамаев М., Петренко С.* Технологии защиты информации Интернета. Специальный справочник. — СПб.: Питер, 2002.

39. *Монин С.* Защита информации и беспроводные сети // КомпьютерПресс. — 2005. — № 4.

40. *Олифер В. Г.* Защита информации при работе в Интернет // Connect. — 2002. — № 11.

41. *Олифер В. Г., Олифер Н. А.* Новые технологии и оборудование IP-сетей. — СПб.: БХВ-Петербург, 2000.

42. *Олифер Н. А.* Дифференцированная защита трафика средствами IPSec // LAN.— 2001. — № 4.

43. *Олифер Н. А.* Протоколы IPSec // LAN. — 2001. — № 3.

44. *Панасенко С. П.* Протоколы аутентификации // BYTE. — 2005. — № 4.

45. *Панасенко С. П., Батура В. П.* Основы криптографии для экономистов: учеб. пособие. — М.: Финансы и статистика, 2005.

46. *Панасенко С. П., Петренко С. А.* Криптографические методы защиты информации для российских корпоративных систем // Конфидент. — 2001. — № 5. — С. 64—71.

47. *Пахомов С.* RAID-массивы — надежность и производительность // КомпьютерПресс. — 2002. — № 3.

48. *Петренко С. А.* Построение эффективной системы антивирусной защиты // Конфидент. — 2002. — № 3.

49. *Петров А. А.* Компьютерная безопасность: криптографические методы защиты. — М.: ДМК Пресс, 2000.

50. Программно-аппаратные средства обеспечения информационной безопасности. Защита программ и данных: учеб. пособие для вузов / П. Ю. Белкин, О. О. Михальский, А. С. Першаков и др. — М.: Радио и связь, 1999.

51. *Проскурин В. Г., Крутов С. В., Мацкевич И. В.* Программно-аппаратные средства обеспечения информационной безопасности. Защита в операционных системах: учеб. пособие для вузов. — М.: Радио и связь, 2000.

52. *Прохоров А.* Windows Vista для домашних пользователей. Ч. 2 // КомпьютерПресс. — 2006. — № 11.

53. *Прохоров А.* Опять про спам // КомпьютерПресс. — 2006. — № 10.

54. Решения компании Cisco Systems по обеспечению безопасности корпоративных сетей / сост.: М. Кадер. — М.: Московский офис Cisco Systems, Inc., 2001.

55. *Романец Ю. В., Тимофеев П. А., Шаньгин В. Ф.* Защита информации в компьютерных системах и сетях. — 2-е изд. — М.: Радио и связь, 2001.

56. *Сабанов А.* Роль аутентификации при обеспечении защищенного удаленного доступа / Компания Aladdin, 2008.

57. *Савченко К.* Российский рынок систем документооборота: прикладные решения // BYTE. — 2008. — № 4 (114).

58. *Садердинов А. А., Трайнев В. А., Федулов А. А.* Информационная безопасность предприятия. — М.: Дашков и К°, 2006.

59. *Сарбуков А., Грушо А.* Аутентификация в компьютерных системах // Системы безопасности. — 2003. — № 5 (53).

60. *Симонов С. В.* Методология анализа рисков в информационных системах // Конфидент. — 2001. — № 1.

61. *Скородумов Б.* Безопасность союза интеллектуальных карточек и персональных компьютеров // Мир карточек. — 2002. — № 5—6.

62. *Смирнов С. Н.* Безопасность систем баз данных. — М.: Гелиос АРБ, 2007.

63. *Соколов А. В., Шаньгин В. Ф.* Защита информации в распределенных корпоративных сетях и системах. — М.: ДМК Пресс, 2002.

64. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). — М.: Гостехкомиссия России, 2001.

65. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от НСД к информации. — М.: Гостехкомиссия России, 1992.

66. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. — М.: Гостехкомиссия России, 1997.

67. Теоретические основы компьютерной безопасности: учеб. пособие для вузов / П. Н. Девянин, О. О. Михальский, Д. И. Правиков и др. — М.: Радио и связь, 2000.

68. Типовые решения по применению средств VPN для защиты информационных ресурсов. — СПб.: Конфидент, 2001.

69. Типовые решения по применению технологии межсетевых экранов для защиты информационных ресурсов. — СПб.: Конфидент, 2001.

70. Типовые решения по применению технологии централизованного управления антивирусной защитой предприятия. — СПб.: Конфидент, 2002.

71. *Трифаленков И., Зайцева Н.* Функциональная безопасность корпоративных систем // Открытые системы. — 2002. — № 07—08.

72. *Чеников О.* Особенности применения двухфакторной аутентификации // Информационная безопасность. — 2005. — № 3.

73. *Шаньгин В. Ф.* Защита компьютерной информации. Эффективные методы и средства. — М.: ДМК Пресс, 2008.

74. *Шарков А. Е., Сердюк В. А.* Защита корпоративного почтового документооборота // Сети и системы связи. — 2003. — № 13.

75. *Шрамко В. Н.* Защита компьютеров: электронные системы идентификации и аутентификации // PCWeek/RE. — 2004. — № 12.

76. Interoperability Specification for ICCs and Personal Computer Systems. Part 8. Recommendations for ICC Security and Privacy Devices. Revision 1.0. PC/SC Workgroup, Dec. 1997.

77. ISO 17799. Международный стандарт безопасности информационных систем: пер. с англ. — М., 2002.

78. ISO/IEC 14443-1. Identification Cards — Contactless integrated circuit(s) cards Proximity Cards Part 1: Physical characteristics International Standard. — 15.04.2000.

79. ISO/IEC 14443-2. Identification Cards — Contactless integrated circuit(s) cards Proximity Cards Part 2: Radio frequency power and signal interface International Standard. — 01.07.2001.

80. *Menezes A. J., van Oorschot P. C., Vanstone S. A.* Handbook of Applied Cryptography. CRC Press, 1999.

Интернет-ресурсы

81. Антивирусная защита компьютерных систем. Лаборатория Касперского. ИНТУИТ, 2008 // *http://www.intuit.ru/department/security/antiviruskasp/.*

82. Базовый стандарт организации беспроводных локальных сетей IEEE 802.11 // *http://standards.ieee.org/reading/ieee/std/lanman/802.11-1999.pdf.*

83. *Беляев А. В.* Методы и средства защиты информации // *http://www.citforum.ru/internet/infsecure/its2000_01.shtml.*

84. *Гудилин О.* Проактивность как средство борьбы с вирусами. Infosecurity, 2008 // *http://www.infosecurity.ru/cgi-bin/cart/.*

85. *Джейсон Л.* Работа в корпоративных сетях с ОС Windows Vista // TechNet. — 2006. — № 11. — *http://technet.microsoft.com.*

86. *Касперский Е.* Компьютерные вирусы // *http://www.kaspersky.ru/.*

87. Комплексное управление безопасностью КУБ. Компания Информзащита // *http://www.infosec.ru/products/cube/.*

88. Коротыгин С. Развитие технологии беспроводных сетей: стандарт IEEE 802.11 // *http://www.ixbt.com/comm/wlan.shtml.*

89. *Кузнецов С.* Защита файлов в операционной системе UNIX // *http://www.citforum.ru/database/articles/art_8.shtml.*

90. *Лукацкий А.* Межсетевые экраны // Компьютерра. — 2007. — № 10. — *http://offline.cio-world.ru/2007/65/341131/.*

91. Обзор Windows Vista / Безопасность // *http://www.webdocs.ru/content-494.html.*

92. *Олифер Н. А., Олифер В. Г.* Сетевые операционные системы. Центр информационных технологий // *http://citforum.ru/operating_systems/sos/contents.shtml.*

93. Продукты Kaspersky Open Space Security. Лаборатория Касперского // *http://www.kaspersky.ru/kaspersky_open_space_security.*

94. Решение ЭЛВИС-ПЛЮС по созданию подсистемы защиты от воздействия вредоносных программ и вирусов // *http://www.elvis.ru/solutions_system.shtml.*

95. Решения CISCO для обеспечения информационной безопасности // *http://www.cisco.com/ru.*

96. Решения IBM для обеспечения информационной безопасности // *http://www.ibm.com/ru.*

97. Решения компании Информзащита. Защищенный доступ к базам данных // *http://www.infosec.ru/sitemap/.*

98. Решения по построению систем ИБ. УЦСБ // *http://www.ussc.ru/index.php.*

99. Руководство по безопасности для системы Windows Vista. Обзор. Microsoft // TechNet. — 2007. — *http://technet.microsoft.com/ru-ru/windows/aa905062.aspx.*

100. *Самодуров А.* Особенности защиты электронного документооборота // CNews Analytics. — 2006. — *http://www.cnews,ru/reviews/free/security 2006/articles/e-docs/.*

101. Семейство продуктов CSP VPN. Компания «С-Терра СиЭсПи», 2008 // *http://www.s-terra.com/index.htm.*

102. Семейство стандартов IEEE 802.11 // *http://www.wireless.ru/wireless/wrl_base80211.*

103. Система электронного документооборота DIRECTUM // *http://www.directum.ru/314838.shtml.*

104. *Скородумов Б. И.* Стандарты для безопасности электронной коммерции в сети Интернет // *http://www.stcarb.comcor.ru.*

105. Электронный документооборот // *http://www.directum-journal.ru/.*

106. FIPS Publication 197. Announcing the Advanced Encryption Standard (AES). — Nov. 2001 // *csrc.nist.gov/publications/fips/fipsl97/fips-197.pdf.*

107. RFC 1928: SOCKS Protocol Version 5 / M. Leech, M. Ganis, Y. Lee etc. — March 1996 // *www.ietf.org/rfc/rfcl928.txt.*

108. RFC 2311: S/MIME Version 2 Message Specification / S. Dusse, P. Hoffman, B. Ramsdell etc. — March 1998 // *www.ietf.org/rfc/rfc231 l.txt.*

Предметный указатель

A

Access Control List *298*

C

Controlled Access Protection Profile *289*
Cookie *193*
Строгая аутентификация *175*

D

DIRECTUM *234*
  архитектура *237*
  ввод и преобразование документов *242*
  жизненный цикл и версии документов *245*
  коллективная работа с документами *247*
  модули *236*
  обеспечение конфиденциальности документов *246*
  поиск документов *244*
  создание и редактирование документов *245*
  управление электронными документами *241*
  функциональность *235*
  хранение документов *243*
  ЭЦП *246*

E

Electronic Document Management Systems *200*
Enterprise Content Management *200*

I

IP-адрес *41*
IP-пакет *43*

K

Kaspersky Open Space Security *512*
  Kaspersky Business Space Security *513*
  Kaspersky Enterprise Space Security *513*
  Kaspersky Total Space Security *513*
  Kaspersky Work Space Security *513*
Kerberos *469*

M

MAC-код *343*

P

PIN-код *160, 173*
  вероятность угадывания *174*
  генерация *174*

R

RAID *218*
  зеркальная копия *219*
  уровни *219*

S

SecurID *378*
Security Policy Processor *532*
SMLT (Stateful Multi-Layer Technique) *389*
SOCKS-клиент *365*
SOCKS-сервер *365*
  функции *366*
SSL-аутентификация *362*
SSL-сессия *361*

T

TACACS *466*

U

UNIX *288*
  syslog-демон *299*
  авторизация доступа *295*
  администраторы *290*
  аудит *299*
  безопасный пароль *291*

домашний каталог пользователя *295*
журнал регистрационной информации *299*
защита на уровне сети *302*
защита файлов от несанкционированного доступа *297*
защита файловой системы *293*
идентификация и аутентификация *291*
индекс *293*
каталог *294*
командный интерпретатор rsh *292*
механизм контроля в режиме ядра *301*
составное имя *294*
списки управления доступом *298*
USB-токен *171*

V

VPN (Virtual Private Network *228*
VPN (Virtual Private Network) *325, 407*
CSP VPN *434*
VPN-клиент *409*
VPN-сервер *409*
авторизация *418*
архитектура *426*
аутентификация *417*
безопасность периметра сети *419*
внутрикорпоративные сети *424*
концепция построения *407*
критерии безопасности данных *416*
локальная сеть *429*
межкорпоративные сети *425*
межсетевые взаимодействия *437*
модуль NME-RVPN *435*
на канальном уровне OSI *325, 423*
на основе маршрутизаторов *425*
на основе межсетевых экранов *425*
на основе программного обеспечения *425*
на основе специализированных аппаратных средств *426*
на сеансовом уровне OSI *359, 424*
на сетевом уровне OSI *335, 423*
ролевое управление доступом *418*
сети с удаленным доступом *424*
система предотвращения вторжений *419*
техническая реализация *430*
угрозы безопасности *408*
управление безопасностью *420*
шлюз безопасности VPN *410*

W

Windows Vista *303*
аппаратные средства защиты *304*
безопасность Internet Explorer 7 *314*
защита данных от утечек и компрометации *312*
защита доступа к сети *306*
защита драйверов *305*
защита от атак на системные службы *305*
защита от вредоносных программ *308*
защита пользовательских данных *314*
защищенный режим IE7 *315*
контроль USB-устройств *314*
контроль над расширениями IE7 *315*
междоменные сценарии *319*
межсетевой экран Windows Firewall *309*
новая версия стека TCP/IP *320*
обеспечение безопасности сети *321*
опознание некорректных URL *317*
подтверждение ActiveX *318*
система шифрования файлов *313*
средства защиты от фишинга *319*
строка состояния безопасности *317*
технология InfoCard *316*
уничтожение истории посещения сайтов *318*
управление параметрами безопасности IE7 *316*
управление учетными записями пользователей *306*
упрощение управления сетью *323*
Центр безопасности Windows *310*
шифрование жесткого диска *313*
WLAN *369*
World Wide Web *36*

A

Автоматизированная система обработки информации *17*
компоненты *18*
Авторизация *20, 159*
Агент системы *446*
Адекватная политика безопасности ОС *274*
оптимальная *275*
этапы формирования и поддержания *275*
Администратор базы данных *214*
Администратор защиты *20*
Администрирование *159*
Алгоритм HMAC *349*

структура *349*
Алгоритмы ЭЦП *130*
DSA *130*
ГОСТ Р 34.10-2001 *132*
ГОСТ Р 34.10-94 *131*
ECDSA *131*
Анализ рисков *77*
Антивирус *502*
дополнительные средства защиты *507*
карантин *504*
модуль обновления *502*
модуль планирования *503*
модуль управления *503*
проверка в режиме реального времени *504*
проверка по требованию *505*
тестирование *505*
Антивирусная база *498*
Антивирусная защита *266, 497*
проактивные методы *499*
сигнатурный анализ *497*
эвристические методы *499*
Антивирусный комплекс *506*
Архитектура безопасности *79*
административные полномочия *81*
защита ресурсов *80*
логическая безопасность *80*
физическая безопасность *79*
протокола L2TP *330*
Архитектура
протокола PPTP *327*
средств безопасности IPSec *338*
Атака *20*
DDoS *266*
захват ресурсов *272*
кража ключевой информации *272*
маскарад *26*
перехват паролей *25*
подбор пароля *271*
полного перебора *50*
превышение полномочий *272*
программные закладки *272*
сборка мусора *272*
сканирование файловой системы *271*
Аудит *286*
Аудит
безопасности информационной системы *533*
политика *288*
требования *287*
Аудитор *287*
Аутентификация *20, 158*
биометрическая *183*
взаимная *159*
категории *160*
междоменная *477*
на основе одноразовых паролей *450*
простая *162*
строгая *166*
схема однократного входа SSO *188*
типы *161*

Б

База данных *211*
База данных MIB *41*
База данных
безопасных ассоциаций SAD *337, 353*
закрытая система *214*
защищенный доступ *225*
открытая система *214*
политик безопасности SPD *337, 353*
Базовая политика безопасности *70*
Безопасная ассоциация SA *339, 352*
Безопасность беспроводной сети *368*
VPN-агенты *372*
защита пользовательских устройств *371*
мониторинг сети *372*
правильная настройка *371*
протокол WEP *369*
стандарт 802.11i *369*
стандарт WPA *369*
традиционные меры *371*
физическая защита *371*
Безопасность операционных систем *270*
UNIX *288*
Windows Vista *303*
административные меры защиты *273*
классификация угроз *270*
комплексный подход *273*
политика безопасности *274*
типичные атаки *271*
фрагментарный подход *272*
Беспроводная локальная сеть WLAN *35*
точка доступа *53*
уязвимости и угрозы *54*
Беспроводная сеть *368*
базовый набор служб BSS *368*
метод прямой последовательности DSSS *369*

расширенный набор служб ESS *368*
режим клиент/сервер *368*
режим точка—точка *368*
точка доступа AP *368*
Биометрическая аутентификация *183*
дактилоскопические системы *184*
мобильные системы *188*
по лицу и голосу *186*
по радужной оболочке и сетчатке глаз *187*
по форме ладони *186*
шифрование *188*
эталонный идентификатор пользователя *184*
эффективность *184*
Блочный симметричный алгоритм *106*
обратная связь по выходу *109*
обратная связь по шифртексту *108*
сцепление блоков шифра *107*
электронная кодовая книга *106*

В

Виртуальный защищенный канал *325, 408*
основные схемы *413*
по протоколу SOCKS *365*
по протоколу SSL *361*
способы построения *355*
Владелец информации *19*
Владелец объекта доступа *279*
Вредоносные программы
компьютерный вирус *26, 492*
подсистема защиты *266*
сетевой червь *27, 493*
троянский конь *26, 494*

Г

Глобальная политика безопасности *524*
правила *526*
Глобальное управление безопасностью GSM *519*
агент безопасности *527*
консоль управления *528*
структурная схема *527*
центр управления *528*
ГОСТ Р 34.10-2001 *132*
ключ подписи *134*
ключ проверки *134*
механизм ЭЦП *134*
параметры схемы ЭЦП *134, 135*
проверка ЭЦП *134, 137*
формирование ЭЦП *134, 136*

Д

Дайджест сообщения *123*
Дайджест-функция *339, 349*
Двоичные векторы *136*
Дейтаграмма *41*
Доверенная вычислительная база *270*
Документы RFC *38*
Домен безопасности *281*
Домен интерпретации DOI *330, 340*
Допустимый временной интервал задержки *162*
Достоверность информации *19*
Доступ к информации *19*
несанкционированный *19*
оперативность *19*
правило *19*
право *19*
санкционированный *19*
субъект *19*
Доступность данных *19*

Ж

Журнал аудита *286*

З

Задача дискретного логарифмирования *114*
Защита базы данных *211*
Microsoft Access 2000 *221*
Oracle *222*
авторизация пользователей *213*
ведение журнала *218*
меры *226*
методы и средства *213*
поддержка целостности данных *217*
потенциальные опасности *211*
права владения *214*
представление *215*
привилегии *214*
применение RAID-массивов *218*
резервное копирование и восстановление *217*
угрозы *212*
шифрование данных *216*
Защита информации *16, 249*
задачи *60*

категорирование *18*
контроль эффективности *266*
методы и средства *60*
непрерывность функционирования средств защиты *268*
объект *16*
от вредоносных программ *27, 510*
от непреднамеренного воздействия *17*
от несанкционированного воздействия *17*
от несанкционированного доступа *17*
от разглашения *17*
от утечки *17*
система *17*
способ *20*
средство *21*
техника *21*
технологии *14*
цель *16*
эффективность *16*
эшелонированная оборона от угроз *250*
Защита электронного документооборота *205*
DIRECTUM *234*
аутентификация *207*
безопасный доступ *207*
законодательное и нормативное регулирование *210*
комплексный подход *205, 210*
конфиденциальность информации *208*
обеспечение подлинности документов *209*
почтового *227*
протоколирование действий пользователей *210*
разграничение прав доступа *208*
сохранность документов *207*
средства *207*
Защищенная операционная система *272*
Защищенная система *20*

И

Идентификатор *20, 158*
Идентификатор набора сервисов SSID *53*
Идентификация *20, 158*
подсистема управления *262*
Изолированная программная среда *283*
Имитоприставка *90, 101*
Инвариант эллиптической кривой *120*
Инкапсуляция *43, 410*
Интернет *35*
интернет-сервисы *36*
основные воозможности *36*
Интранет *36*
Информационная безопасность *3, 17, 57, 249*
основные области *59*
Инфраструктура управления открытыми ключами PKI *146*
дополнительные компоненты *154*
защита от атаки «человек-в-середине» *147*
иерархия *151*
каталог сертификатов *152*
основные задачи *150*
поддерживающие приложения и стандарты *156*
подсистемы комплексной системы обеспечения безопасности *155*
процедура проверки ЭЦП *152*
стандарт X.509 *151*
структура *152*
уровни *154*
функции *153*
центр регистрации RA *153*
центр сертификации CA *153*
Инцидент информационной безопасности *267*
ИТ-угрозы *32*

К

Канальный посредник *385*
Каталог открытых ключей PKD *154*
Ключ шифрования *87, 90, 111*
временный (сеансовый) *355*
общий сессионный *143*
основной *354*
открытый *89*
секретный *89*
Ключ-сертификат *149*
Код аутентификации сообщения *108, 124*
Код проверки целостности ICV *343*
Комплекс средств защиты *21*
Консорциум ISTF *59*
Конфиденциальность данных *18, 85*
Концентратор доступа LAC *332*
Корневой сертификат *152*
Корпоративная информационная система *15, 249*
архитектура *250*
общие требования *13*
структурная схема *252*

Криптограмма *87*
Криптографическая защита *261*
Криптографическая защита информации *86*
Криптографическая контрольная сумма *124*
Криптографический алгоритм *88*
3-DES *97*
AES *102*
Blowfish *106*
DES *94*
ECES *122*
IDEA *105*
RC2 *105*
RC5 *105*
RSA *116*
ГОСТ 28147-89 *98*
комбинирование *96*
симметричный *91*
стойкий *92*
Криптография *86*
Криптосистема *88*
асимметричная *111*, *115*
комбинированная *139*
на базе эллиптических кривых *120*
симметричная *90*
схема *87*

Л

Локальная политика безопасности *527*

М

Мандаты возможностей *282*
Маршрутизатор *37*
Матрица доступа *260*, *281*, *282*
Матрица ключей *91*
Международный институт стандартов ISO *37*
Межсетевой экран *251*, *265*, *373*
Cisco IOS Firewall *403*
Cisco Pix Firewall *403*
администрирование *380*
задачи *392*
идентификация и аутентификация *378*
классификация *374*
основные задачи *373*
персональный *401*
политика межсетевого взаимодействия *392*
прикладной шлюз *386*
программно-аппаратный *391*
программный *390*
распределенный *402*
регистрация событий *381*
схемы подключения *395*
тенденции развития *404*
трансляция сетевых адресов *379*
фильтрация трафика *374*
функции посредничества *376*
шлюз сеансового уровня *384*
шлюз экспертного уровня *389*
экранирующий маршрутизатор *383*
Метод доступа *278*
Метод комплексной защиты конфиденциальности и аутентичности данных *144*
схема работы *144*
Метод открытого распределения ключей Диффи — Хеллмана *139*, *142*
Механизм трансляции сетевых адресов NAT *344*
Модели разграничения доступа *280*, *286*
избирательное разграничение доступа *280*
изолированная программная среда *283*
полномочное разграничение доступа с контролем потоков *284*
Модель ISO/OSI *37*
обмен данными *38*
протоколы *38*
уровни *38*, *39*
Модель нарушителя *24*
Модульная экспонента с фиксированными основанием и модулем *114*
Монитор ссылок *279*
Мониторинг безопасности информационной системы *536*

Н

Надежная система *290*
Нарушение целостности данных *212*
Неприкосновенность данных *212*
Несанкционированный доступ *25*
незаконное использование привилегий *26*
основные каналы *25*
система защиты *260*

О

Обеспечение безопасности сетей *56*

комплексный подход *56*
меры защиты *57*
фрагментарный подход *56*
Обеспечение совместимости *37*
Обнаружение вторжений *265, 479*
Объект доступа *278*
Объект системы *18*
Однонаправленная функция *113*
Оранжевая книга *289, 550*
Орган сертификации CA *352*
Открытая подсеть *396*

П

Пакетный фильтр *383*
Пароль *160*
динамический (одноразовый) *160*
передача и хранение *164*
Персональный идентификационный номер PIN *160*
Поведенческий блокиратор *500*
Подлинность информации *85*
Подсистема защиты ОС *276*
авторизация *277*
аудит *286*
аутентификация *277*
идентификация *277*
криптографические функции *276*
разграничение доступа *278*
сетевые функции *276*
управление политикой безопасности *276*
Подсистема управления идентификацией и доступом IAM *159, 196*
Политика безопасности *21, 56, 62*
верхний уровень *65*
дополнительная информация *64*
команда по разработке *76*
нижний уровень *66*
область применения *63*
описание проблемы *63*
основные положения *70*
по умолчанию *526*
позиция организации *64*
распределение ролей и обязанностей *64*
санкции *64*
составление *78*
средний уровень *66*
структура *69*
требования *76*
управленческие меры *69*
установление уровня безопасности *78*
этапы программы *75*
Полосовое распределение данных *219*
Пользователь информации *19*
Потеря доступности данных *212*
Похищение и фальсификация данных *211*
Почтовая система документооборота *227*
антивирусная защита *232*
архитектура *227*
защита от утечки информации *232*
защита передаваемых данных *228*
защита почтовых серверов *231*
комплексная защита *233*
криптографическая защита *230*
обеспечение конфиденциальности и целостности данных *229*
Правило NRU *284*
Правило NWD *285*
Право доступа к объекту *279*
Предотвращение вторжений *265, 479*
Привилегия *222*
на объект *223*
роли *224*
системная *223*
Проблема дискретного логарифма эллиптической кривой ECDLP *122*
Проблема многих входов *189*
Программный посредник *387*
Программы-посредники *364, 376*
функции *376*
Прокси-сервер *377*
Простая аутентификация *162*
на основе многоразовых паролей *163*
на основе одноразовых паролей *165*
процедура *163*
схема *163*
атаки *161*
Протокол аутентификации
на основе асимметричных алгоритмов *181*
на основе однонаправленных ключевых хэш-функций *178*
на основе симметричных алгоритмов *177*
на основе цифровой подписи *182*
одноразовые параметры *176*
предотвращение атак *161*
PAP *163*
характеристики *162*
Протокол
AH *341*

CHAP *455*
EAP *369, 458*
EAP-TLS *327*
ESP *344*
IKE *337, 351*
IPSec *335, 561*
ISAKMP *340, 351*
IKE *338*
L2F *329*
L2TP *329*
LCP *326*
MSCHAP *327*
NCP *326*
PPP *326*
S/Key *461*
SET *561*
SMTP *204*
SOAP *205*
SOCKS *364*
SSL *360, 561*
TKIP *369*
TLS *362*
UDP *331*
АН *339*
ESP *339*
ECKEP *145*
PAP *327, 454*
PPP *449*
PPTP *326*
Процедуры безопасности *73*
реагирования на события *74*
управления конфигурацией *74*

Р

Рабочая станция *506*
Разграничение доступа *279*
избирательное *280*
полномочное *280, 284*
правила *279*
Режимы протокола АН *343*
транспортный *343*
туннельный *344*
Режимы протокола ESP *346*
транспортный *346*
туннельный *347*
Резервное копирование *217, 268*
Ресурсы системы *20*
доступность *20*
целостность *20*
Решение задач ААА *159*
Роли и ответственности в безопасности *224*
Роли и ответственности в безопасности сети *81*
аудит и оповещение *82*
тревожная сигнализация *83*

С

Сервис удаленного доступа RAS *329*
Сертификат открытого ключа *148*
генерация пары ключей *150*
свойства *150*
составляющие *150*
формирование *149*
Сертификация открытого ключа *149*
Сетевая система NIPS *480*
Сетевая атака *45*
IP-спуфинг *47*
анализ сетевого трафика *47*
злоупотребление доверием *51*
изменение данных *47*
криминализация *52*
на уровне приложений *50*
отказ в обслуживании *49*
парольная *49*
перехват пароля *47*
перехват сеанса *48*
подмена доверенного субъекта *47*
подслушивание *46*
посредничество *48*
причины *52*
угадывание ключа *50*
удаленная *46*
цели *46*
«человек-в-середине» *48*
Сетевая разведка *51*
Сетевой сервер LNS *332*
Сеть Фейстеля *93*
Сигнатура атаки *483*
Сигнатура вируса *498*
Система активного мониторинга *232*
Система бесперебойного питания *268*
Система запрос—ответ *160*
Система защиты информации КИС
меры и средства *258*
общая структура *259*
общие требования *257*
подсистемы *260*
структурная схема *255*

Система информационной безопасности КИС *252*
санкционированный доступ *253*
функции *254*
Система предотвращения вторжений IPS *479*
защита от DDoS-атак *488*
методы анализа *482*
обнаружение аномального поведения *482*
обнаружение злоупотреблений *483*
предотвращение вторжений сетевого уровня *485*
предотвращение вторжений системного уровня *484*
признаки *480*
функции *483*
Система управления доступом *442*
веб-доступом *447*
сетевым *446*
функционирование *445*
Система управления средствами информационной безопасности *516*
Cisco IP Solution Center (ISC) *542*
Cisco Monitoring, Analysis and Response System (MARS) *541*
Cisco Security Manager (CSM) *540*
IBM Proventia Management SiteProtector *547*
IBM Tivoli *543*
вертикальная структура *519*
задачи *516*
ЗАСТАВА *538*
инцидент информационной безопасности *536*
разграничение доступа к сетевому оборудованию *521*
управление конфигурациями *520*
управление обновлениями программных средств *519*
функции управления GSM *531*
характеристики *530*
Система электронного документооборота *200*
автоматизация управления рабочими процессами *202*
идентификация и аутентификация *202*
подсистемы *202*
разграничение прав пользователей *202*
реализация обмена данными *204*
регистрация событий *203*
схема с равноправными серверами *204*
угрозы *206*
управление электронными документами *203*
централизованная схема *203*
Сканеры уязвимости *480*
Смарт-карта *168*
бесконтактная *168*
генерация ключей *170*
интеллектуальная *171*
контактная *168*
Снижение рисков *264*
Сниффер пакетов *46*
Собственник информации *19*
Событие информационной безопасности *267*
Соксификатор *366*
Спам *509*
антиспамовый фильтр *509*
подсистема защиты *266*
Специализированная политика безопасности *70*
допустимого использования *71*
удаленного доступа *72*
Списки отмененных сертификатов CRL *153*
Список прав доступа ACL *282*
Стандарт X/Open Single Sign-On (XSSO) *195*
Стандарт
802.11 *368*
BSI *553*
IEEE 802.11 *556*
ISO 15408 *289*, *553*
ISO/IEC 17799\:2000 (BS 7799\:2000) *551*
WPA *369*
ГОСТ Р ИСО/МЭК 15408 *289*, *565*
информационной безопасности *549*
Стандартизация *37*
Стек коммуникационных протоколов *38*
Стек протоколов IPSec *335*, *348*
AH *338*
ESP *338*
IKE *338*
архитектура *338*
компоненты *337*
криптографические технологии *336*
основные задачи *337*
преимущества *358*
схемы применения *357*
Стек протоколов ISO/OSI *38*
Стек протоколов TCP/IP *38*
Frame Relay *42*

FTP *40*
ICMP *42*
IP *41*
OSPF *42*
PPP *42*
RIP *42*
SLIP *42*
SNMP *41*
TCP *41*
Telnet *40*
TFTP *40*
UDP *41*
X.25 *42*
свойства *39*
структура *39*
Строгая аутентификация *166*
двусторонняя *166*
двухфакторная *167*
на основе асимметричных алгоритмов *181*
на основе симметричных алгоритмов *177*
односторонняя *166*
трехсторонняя *167*
Структура пакета
IP *336*
L2TP *331*
PPTP *327*
Субъект доступа *278*
суперпользователь *279*
Субъект системы *18*
Схема SSO (Single Sign-On) *188*
IBM Global Sign-On for Multiplatforms (GSO) *194*
Web SSO *192*
автоматизация *190*
продукты уровня предприятия *194*
Схема туннелирования
по протоколу PPTP *328*
по протоколу L2TP *332*
Схемы подключения межсетевых экранов *395*
единой защиты локальной сети *397*
с защищаемой закрытой и не защищаемой открытой подсетями *397*
с использованием экранирующего маршрутизатора *395*
с несколькими сетевыми интерфейсами *396*
с раздельной защитой закрытой и открытой подсетей *398*

Т

Терминальный сервер *399*
Токен безопасности *151*
Точки эллиптической кривой *120*
Трансляция сетевых адресов NAC *262*
Туннелирование *347*, *410*
Туннель VPN *325*, *409*
защита информации *409*
инициатор туннеля *415*
терминатор туннеля *415*

У

Угроза безопасности *20*, *21*
классификация *22*
основные виды *29*, *30*
основные методы реализации *31*
преднамеренная *24*
случайные воздействия *24*
спам *27*
фарминг *29*
фишинг *28*
Удаленный доступ *448*
аутентификация *450*
достоинства *449*
методы управления *443*
протокол Kerberos *469*
протокол PPP *449*
протоколы аутентификации *454*
сервер аутентификации *465*
сервер удаленного доступа *449*
система TACACS *467*
уровни управления *444*
централизованный контроль *464*
Универсальный веб-агент UWA *447*
Управление доступом *196*
модель ролевого управления *197*
подсистема управления учетными записями *197*
схема однократного входа SSO *189*
централизованное *198*
Управление криптоключами *138*
задачи *146*
ключевая информация *138*
протокол распределения ключей *138*
прямой обмен ключами *139*
распределение ключей *138*
Управление рисками *254*
централизованное *255*

Уровни доступа *31*
Ущерб безопасности *20*
Уязвимость компьютерной системы *20*

Ф

Фильтрация трафика *374*
  критерии анализа *375*
  правила фильтрации *375*
  с контролем состояния соединения *389*
Формат заголовка
  AH *342*
  ESP *345*
Функции безопасности протокола SSL *363*

Х

Хост *36*
Хостовая система HIPS *480*
Хэширование *88*
Хэш-функция
  MD *124*
  SHA *125*
  ГОСТ Р 34.11-94 *125*
  односторонняя *124*
  свойства *123*

Ц

Целостность информации *18, 85*
Центр сертификации CA *149*
  схема работы *153*

Ч

Частично защищенная операционная система *272*

Ш

Шифр
  перемешивание *93*
  рассеивание *92*
  составной *93*
Шифрование данных *87*
  асимметричное *89*
  блочное *89*
  многократное *96*
  поточное *89*
  прозрачное *216*
  с явным заданием ключа пользователем *216*
  симметричное *89*
Шлюз *37*
  безопасности *346*
  экранирующий *386*

Э

Эвристический анализатор *499*
Электронная цифровая подпись *89, 126*
  достоинства *126*
  процедура проверки *128*
  процедура формирования *127*
  секретный ключ *128*
  структура *129*
Электронный документ *242*
Электронный документооборот *200*
  преимущества *201*
  распределенный *203*

Ю

Юридическая значимость информации *19*

Оглавление

Предисловие 3

Список сокращений 7

Введение 12

ЧАСТЬ I. ПРОБЛЕМЫ БЕЗОПАСНОСТИ КОРПОРАТИВНОЙ ИНФОРМАЦИИ 15

Глава 1. ОСНОВНЫЕ ПОНЯТИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 16

1.1. Основные понятия защиты информации и информационной безопасности 16
1.2. Анализ угроз информационной безопасности 21

Глава 2. ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СЕТЕЙ 35

2.1. Введение в сетевой информационный обмен 35
2.1.1. Использование сети Интернет 35
2.1.2. Модель ISO/OSI и стек протоколов TCP/IP 37
2.2. Анализ угроз сетевой безопасности 44
2.2.1. Проблемы безопасности IP-сетей 45
2.2.2. Угрозы и уязвимости беспроводных сетей 53
2.3. Обеспечение информационной безопасности сетей 56
2.3.1. Способы обеспечения информационной безопасности 56
2.3.2. Пути решения проблем защиты информации в сетях . . 59

Глава 3. ПОЛИТИКА БЕЗОПАСНОСТИ 62

3.1. Основные понятия политики безопасности 63
3.2. Структура политики безопасности организации 69
3.2.1. Базовая политика безопасности 70
3.2.2. Специализированные политики безопасности 70
3.2.3. Процедуры безопасности 73
3.3. Разработка политики безопасности организации 75

ЧАСТЬ II. ТЕХНОЛОГИИ ЗАЩИТЫ КОРПОРАТИВНЫХ ДАННЫХ 85

Глава 4. КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ 86

4.1. Основные понятия криптографической защиты информации 86
4.2. Симметричные криптосистемы шифрования 90
4.2.1. Алгоритмы шифрования DES и 3-DES 94
4.2.2. Стандарт шифрования ГОСТ 28147—89 98
4.2.3. Американский стандарт шифрования AES 102
4.2.4. Основные режимы работы блочного симметричного алгоритма 106
4.2.5. Особенности применения алгоритмов симметричного шифрования 110
4.3. Асимметричные криптосистемы шифрования 111
4.3.1. Алгоритм шифрования RSA 116
4.3.2. Асимметричные криптосистемы на базе эллиптических кривых 120
4.3.3. Алгоритм асимметричного шифрования ECES 122
4.4. Функция хэширования 123
4.5. Электронная цифровая подпись 126
4.5.1. Основные процедуры цифровой подписи 126
4.5.2. Алгоритм цифровой подписи DSA 130
4.5.3. Алгоритм цифровой подписи ECDSA 131
4.5.4. Алгоритм цифровой подписи ГОСТ Р 34.10—94 131
4.5.5. Отечественный стандарт цифровой подписи ГОСТ Р 34.10—2001 132
4.6. Управление криптоключами 138
4.6.1. Использование комбинированной криптосистемы 139
4.6.2. Метод распределения ключей Диффи — Хеллмана . . . 142
4.6.3. Протокол вычисления ключа парной связи ECKEP . . 145
4.7. Инфраструктура управления открытыми ключами PKI 146
4.7.1. Принципы функционирования PKI 147
4.7.2. Логическая структура и компоненты PKI 150

Глава 5. ИДЕНТИФИКАЦИЯ, АУТЕНТИФИКАЦИЯ И УПРАВЛЕНИЕ ДОСТУПОМ 158

5.1. Аутентификация, авторизация и администрирование действий пользователей 158
5.2. Методы аутентификации, использующие пароли 162
5.2.1. Аутентификация на основе многоразовых паролей . . . 163
5.2.2. Аутентификация на основе одноразовых паролей 165
5.3. Строгая аутентификация 166

5.3.1. Основные понятия 166
5.3.2. Двухфакторная аутентификация 167
5.3.3. Криптографические протоколы строгой аутентификации 175
5.4. Биометрическая аутентификация пользователя 183
5.5. Управление доступом по схеме однократного входа с авторизацией Single Sign-On 188
5.5.1. Простая система однократного входа Single Sign-On 190
5.5.2. Системы однократного входа Web SSO 192
5.5.3. SSO-продукты уровня предприятия 194
5.6. Управление идентификацией и доступом 196

Глава 6. ЗАЩИТА ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА 200

6.1. Концепция электронного документооборота 200
6.2. Особенности защиты электронного документооборота 205
6.3. Защита баз данных 211
6.3.1. Основные типы угроз 212
6.3.2. Методы и средства защиты СУБД 213
6.3.3. Средства защиты СУБД Microsoft Access 221
6.3.4. Средства защиты СУБД Oracle 222
6.3.5. Защищенный доступ к базам данных 225
6.4. Защита корпоративного почтового документооборота 227
6.4.1. Защита каналов сетевого взаимодействия почтовых клиентов и серверов 228
6.4.2. Обеспечение конфиденциальности и целостности электронных документов 229
6.4.3. Обеспечение работоспособности почтовых серверов 231
6.4.4. Обеспечение антивирусной защиты почтовой системы 232
6.4.5. Защита от утечки конфиденциальной информации 232
6.4.6. Комплексный подход к защите корпоративной почтовой системы 233
6.5. Защита системы электронного документооборота DIRECTUM 234
6.5.1. Функциональность системы DIRECTUM 235
6.5.2. Архитектура системы DIRECTUM 237
6.5.3. Управление электронными документами в системе DIRECTUM 241

ЧАСТЬ III. КОМПЛЕКСНАЯ ЗАЩИТА КОРПОРАТИВНЫХ ИС 249

Глава 7. ПРИНЦИПЫ КОМПЛЕКСНОЙ ЗАЩИТЫ КОРПОРАТИВНОЙ ИНФОРМАЦИИ 250

7.1. Архитектура корпоративной информационной системы 250
7.2. Структура системы защиты информации в корпоративной информационной системе 254
7.3. Комплексный подход к обеспечению информационной безопасности КИС 257
7.4. Подсистемы информационной безопасности КИС 260

Глава 8. БЕЗОПАСНОСТЬ ОПЕРАЦИОННЫХ СИСТЕМ 270

8.1. Проблемы обеспечения безопасности ОС 270
8.1.1. Угрозы безопасности операционной системы 270
8.1.2. Понятие защищенной операционной системы 272
8.2. Архитектура подсистемы защиты операционной системы . . . 276
8.2.1. Основные функции подсистемы защиты операционной системы 276
8.2.2. Идентификация, аутентификация и авторизация субъектов доступа 277
8.2.3. Разграничение доступа к объектам операционной системы 278
8.2.4. Аудит 286
8.3. Обеспечение безопасности ОС UNIX 288
8.3.1. Основные положения 288
8.3.2. Парольная защита 291
8.3.3. Защита файловой системы 293
8.3.4. Средства аудита 299
8.3.5. Безопасность системы UNIX при работе в сети 302
8.4. Безопасность ОС Windows Vista 303
8.4.1. Средства защиты общего характера 304
8.4.2. Защита от вредоносных программ 308
8.4.3. Защита данных от утечек и компрометации 312
8.4.4. Безопасность Internet Explorer 7 314
8.4.5. Обеспечение безопасности работы в корпоративных сетях 320

Глава 9. ПРОТОКОЛЫ ЗАЩИЩЕННЫХ КАНАЛОВ 325

9.1. Защита на канальном уровне — протоколы PPTP, L2F и L2TP 325
9.1.1. Протокол PPTP 326
9.1.2. Протоколы L2F и L2TP 329
9.2. Защита на сетевом уровне — протокол IPSec 335
9.2.1. Архитектура средств безопасности IPSec 336

9.2.2. Защита передаваемых данных с помощью протоколов AH и ESP 341
9.2.3. Протокол управления криптоключами IKE 351
9.2.4. Особенности реализации средств IPSec 356
9.3. Защита на сеансовом уровне — протоколы SSL/TLS и SOCKS 359
9.3.1. Протоколы SSL/TLS 360
9.3.2. Протокол SOCKS 364
9.4. Защита беспроводных сетей 368

Глава 10. МЕЖСЕТЕВОЕ ЭКРАНИРОВАНИЕ 373

10.1. Функции межсетевых экранов 373
10.1.1. Фильтрация трафика 374
10.1.2. Выполнение функций посредничества 376
10.1.3. Дополнительные возможности МЭ 378
10.2. Особенности функционирования межсетевых экранов на различных уровнях модели OSI 382
10.2.1. Экранирующий маршрутизатор 383
10.2.2. Шлюз сеансового уровня 384
10.2.3. Прикладной шлюз 386
10.2.4. Шлюз экспертного уровня 389
10.2.5. Варианты исполнения межсетевых экранов 390
10.3. Схемы сетевой защиты на базе межсетевых экранов 392
10.3.1. Формирование политики межсетевого взаимодействия 392
10.3.2. Основные схемы подключения межсетевых экранов 395
10.3.3. Персональные и распределенные сетевые экраны . . . 400
10.3.4. Примеры современных межсетевых экранов 402
10.3.5. Тенденции развития межсетевых экранов 404

Глава 11. ВИРТУАЛЬНЫЕ ЗАЩИЩЕННЫЕ СЕТИ VPN 407

11.1. Концепция построения виртуальных защищенных сетей VPN 407
11.1.1. Основные понятия и функции сети VPN 408
11.1.2. Варианты построения виртуальных защищенных каналов 413
11.1.3. Средства обеспечения безопасности VPN 416
11.2. VPN-решения для построения защищенных сетей 420
11.2.1. Классификация сетей VPN 421
11.2.2. Основные варианты архитектуры VPN 426
11.2.3. Основные виды технической реализации VPN 430
11.3. Современные отечественные VPN-продукты 433
11.3.1. Семейство VPN-продуктов компании «С-Терра СиЭсПи» 434

Глава 12. ЗАЩИТА УДАЛЕННОГО ДОСТУПА 441
12.1. Особенности удаленного доступа 441
12.1.1. Методы управления удаленным доступом 443
12.1.2. Функционирование системы управления доступом . . 445
12.2. Организация защищенного удаленного доступа 448
12.2.1. Средства и протоколы аутентификации удаленных пользователей 450
12.2.2. Централизованный контроль удаленного доступа . . . 464
12.3. Протокол Kerberos 469

Глава 13. ОБНАРУЖЕНИЕ И ПРЕДОТВРАЩЕНИЕ ВТОРЖЕНИЙ 479
13.1. Основные понятия 479
13.2. Обнаружение вторжений системой IPS 482
13.3. Предотвращение вторжений в КИС 484

Глава 14. ЗАЩИТА ОТ ВРЕДОНОСНЫХ ПРОГРАММ И СПАМА 492
14.1. Классификация вредоносных программ 492
14.2. Основы работы антивирусных программ 497
14.2.1. Сигнатурный анализ 497
14.2.2. Проактивные методы обнаружения 499
14.2.3. Дополнительные модули 502
14.2.4. Режимы работы антивирусов 504
14.2.5. Антивирусные комплексы 506
14.2.6. Дополнительные средства защиты 507
14.3. Защита корпоративной сети от воздействия вредоносных программ и вирусов 510
14.3.1. Подсистема защиты корпоративной информации от вредоносных программ и вирусов 511
14.3.2. Серия продуктов «Kaspersky Open Space Security» для защиты корпоративных сетей от современных интернет-угроз 512

Часть IV. УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ 515

Глава 15. УПРАВЛЕНИЕ СРЕДСТВАМИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 516
15.1. Задачи управления информационной безопасностью 516
15.2. Архитектура управления информационной безопасностью КИС 522
15.2.1. Концепция глобального управления безопасностью GSM 523

15.2.2. Глобальная и локальные политики безопасности 524
15.3. Функционирование системы управления информационной безопасностью КИС 527
15.3.1. Назначение основных средств защиты 527
15.3.2. Защита ресурсов 529
15.3.3. Управление средствами защиты 530
15.4. Аудит и мониторинг безопасности КИС 532
15.4.1. Аудит безопасности информационной системы 532
15.4.2. Мониторинг безопасности системы 536
15.5. Обзор современных систем управления безопасностью 538
15.5.1. Централизованное управление безопасностью, реализованное в продуктах «ЗАСТАВА» 538
15.5.2. Программные средства компании Cisco для управления безопасностью сетей 540
15.5.3. Продукты компании IBM для управления средствами безопасности 543

Глава 16. СТАНДАРТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 549

16.1. Роль стандартов информационной безопасности 549
16.2. Международные стандарты информационной безопасности 551
16.2.1. Стандарты ISO/IEC 17799:2002 (BS 7799:2000) 551
16.2.2. Германский стандарт BSI 553
16.2.3. Международный стандарт ISO 15408 «Общие критерии безопасности информационных технологий» 553
16.2.4. Стандарты для беспроводных сетей 556
16.2.5. Стандарты информационной безопасности для Интернета 559
16.3. Отечественные стандарты безопасности информационных технологий 563

Литература 568

Предметный указатель 574

Шаньгин Владимир Федорович

Комплексная защита информации в корпоративных системах

Учебное пособие

Редактор *Е. А. Тульсанова*
Корректор *О. Н. Картамышева*
Компьютерная верстка *И. В. Кондратьевой*
Оформление серии *К. В. Пономарева*

Подписано в печать 22.06.2009. Формат 70×100/16.
Гарнитура «Таймс». Усл. печ. л. 47,73. Уч.-изд. л. 48,2.
Печать офсетная. Бумага офсетная. Тираж 2000 экз.
Заказ № 7037

ЛР № 071629 от 20.04.98
Издательский Дом «ФОРУМ»
101990, Москва — Центр, Колпачный пер., д. 9а
Тел./факс: (495) 625-39-27
E-mail: forum-books@mail.ru

ЛР № 070824 от 21.01.93
Издательский Дом «ИНФРА-М»
127282, Москва, Полярная ул., д. 31в
Тел.: (495) 380-05-40
Факс: (495) 363-92-12
E-mail: books@infra-m.ru
Http://www.infra-m.ru

По вопросам приобретения книг обращайтесь:

Отдел продаж «ИНФРА-М»
127282, Москва, ул. Полярная, д. 31в
Тел.: (495) 363-42-60
Факс: (495) 363-92-12
E-mail: books@infra-m.ru

Центр комплектования библиотек
119019, Москва, ул. Моховая, д. 16
(Российская государственная библиотека, кор. К)
Тел.: (495) 695-93-15

Магазин «Библиосфера» (розничная продажа)
109147, Москва, ул. Марксистская, д. 9
Тел.: (495) 670-52-18, (495) 670-52-19

Отпечатано в ОАО «Можайский полиграфический комбинат»
143200, г. Можайск, ул. Мира, 93.

ШАНЬГИН Владимир Федорович

Доктор технических наук, профессор-консультант кафедры «Информатика и программное обеспечение вычислительных систем» Московского Государственного института электронной техники – технического университета. Действительный член Международной академии информатизации.

Область научных интересов – преобразование, обработка и защита информации в компьютерных системах и сетях. Автор более 150 научных работ, в том числе пяти монографий (в соавторстве) и четырех учебных пособий по информационной безопасности и защите информации в компьютерных системах и сетях (2001 – 2009 г.).

ISBN 978-5-8199-0411-4

9 785819 904114