

Министерство образования РФ

**Санкт-Петербургский государственный электротехнический
университет «ЛЭТИ»**

И. В. ГЕРАСИМОВ, В. А. КАЛМЫЧКОВ, А. В. КОЧЕТКОВ

ИНФОРМАТИКА

**Санкт-Петербург
2001**

Министерство образования РФ

Санкт-Петербургский государственный электротехнический университет
«ЛЭТИ»

И. В. ГЕРАСИМОВ, В. А. КАЛМЫЧКОВ, А. В. КОЧЕТКОВ

ИНФОРМАТИКА

**Учебно–методические комплексы
по теме "Информационная безопасность"**

Санкт-Петербург
Издательство СПбЭТУ «ЛЭТИ»
2001

УДК 621.399
ББК 3973.233я7
Г37

Герасимов И.В., Калмычков В.А., Кочетков А.В. Информатика. Учебно-методический комплекс по теме “Информационная безопасность”: Учеб. пособие. СПб.: Изд-во СПбГЭТУ «ЛЭТИ», 2001. 64 с.

Содержит материалы раздела “Основные положения информационной безопасности” вводного курса учебной дисциплины “Информатика”. Введены основные термины и понятия, представлены общие сведения о существующих угрозах информационной безопасности и приведены данные о возможных мероприятиях по обеспечению защиты информации и корпоративной сети от несанкционированного доступа.

Излагаются основные сведения о компьютерных вирусах и средствах по их обезвреживанию. Включены формулировки статей уголовного кодекса РФ, направленные на защиту информации при использовании компьютерных технологий.

Предназначено для студентов СПбГЭТУ, изучающих дисциплину “Информатика”.

Рецензент: кафедра системотехники и ЭВМ СЗТУ, канд. тех. наук
доц. А.Г. Волков (СПбГТИ)

Утверждено

Редакционно-издательским советом университета
в качестве учебного пособия.

© СПбГЭТУ “ЛЭТИ”, 2001

Введение

В наше компьютеризированное время при наличии быстро развивающихся технологий связи и передачи данных все сложнее становится сохранить в неприкосновенности ту информацию, которая не предназначена для всеобщего использования. Государственные тайны, корпоративные секреты, закрытые сведения из экономики и финансовой деятельности, личная жизнь и многое другое, что фиксируется в разном виде с помощью компьютерной техники, не должны выходить за пределы обозначенного круга их владельцев без соответствующего разрешения или специальной санкции на раскрытие такой информации. Конкурентоспособность предприятий и величина их доходов, независимость стран и жизненный уровень людей зачастую зависят от того насколько удастся им не только воспользоваться научными достижениями и новыми технологиями, но и до определенного времени сохранить в тайне правительственную, коммерческую и конфиденциальную информацию. В противовес этому достаточно развиты различные виды разведки и промышленного шпионажа, включая и компьютерные методы их ведения. Несколько изменив фразу "кто владеет информацией – тот правит миром", можно сказать, что информация правит миром. Преждевременная доступность или исчезновение информации может привести к катастрофическим последствиям. Поэтому возрастает значимость не только средств получения информации, но и средств их надежного хранения и передачи в защищенном режиме, а также технологий защиты корпоративных сетей от несанкционированного доступа к имеющимся ресурсам (аппаратным и программным), угроз потери и искажения циркулирующей в них информации.

В данное издание включен краткий обзорный материал, связанный с лекционным курсом и проблематикой информационной безопасности, рассматривается общий подход к обеспечению защиты информации и включению локальной сети организации в глобальную сеть Интернет, представлены основные способы защиты информации. На страницах пособия представлены способы обеспечения безопасной работы при использовании персонального компьютера и корпоративной сети с учетом опасности компьютерных вирусов и сетевых атак, охарактеризованы основные их виды, а также представлены средства (аппаратные и программные комплексы), предназначенные для отражения наносимого ими вреда.

1. Понятие информационной безопасности.

Защита информации включает в себя комплекс мероприятий, методов и технологий, направленных на обеспечение информационной безопасности (ИБ). На практике под этим достаточно широким спектром понимается поддержание целостности, доступности и, если нужно, конфиденциальности информации и ресурсов, используемых для ввода, хранения, обработки и передачи данных.

Информационная безопасность – это защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, чреватых нанесением ущерба владельцам или пользователям информации и поддерживающей инфраструктуры.

В настоящее время объем средств, затрачиваемых в мире на обеспечение информационной безопасности, составляет более 5 млрд. долларов в год. На

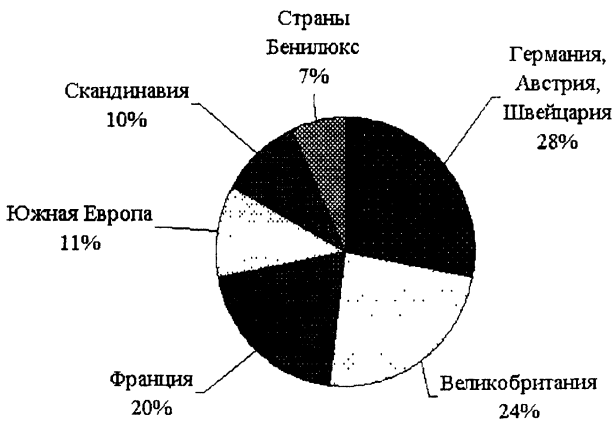


Рис. 1. Доли затрат европейских стран на информационную безопасность в 2001 г.

рис. 1 представлено соотношение затрат на обеспечение ИБ в странах Европы. В то же время общий уровень убытков от нарушений системы ИБ у 500 крупнейших мировых корпораций в 2000 г. по экспертным оценкам составил около 17 млрд. долларов.

В России вопросам, связанным с обеспечением ИБ, и раньше уделялось особое внимание, а в последнее время в связи с широким внедрением компьютерных технологий во многие отрасли производства и управления этой тематике стали уделять все более пристальное внимание.

Российские организации, которые заинтересованы в защите своих информационных ресурсов и поэтому активно использующие в своей деятельности средства ИБ, можно разделить на две основные части:

- 1) в основном государственные учреждения или те предприятия, которым предписано следовать требованиям, инструкциям и руководящим документам ФАПСИ (Федеральное агентство правительственной связи и информации) и других государственных органов;
- 2) коммерческие компании (как крупные промышленно-финансовые группы, так и представители малого бизнеса), которые в различной степени заинтересованы в защите своих корпоративных сетей и локальных сетей своих подразделений или филиалов.

Следует также отметить, что в определенных случаях проблема ИБ как в целом, так и применительно к отдельным организациям может существенным образом затрагивать личные интересы любого человека (например, защита и сохранность информации на персональных картах, эмитированных разными организациями, в частности банками).

Долевое соотношение продаж продуктов и услуг на рынке информационной безопасности России показаны на рис. 2.

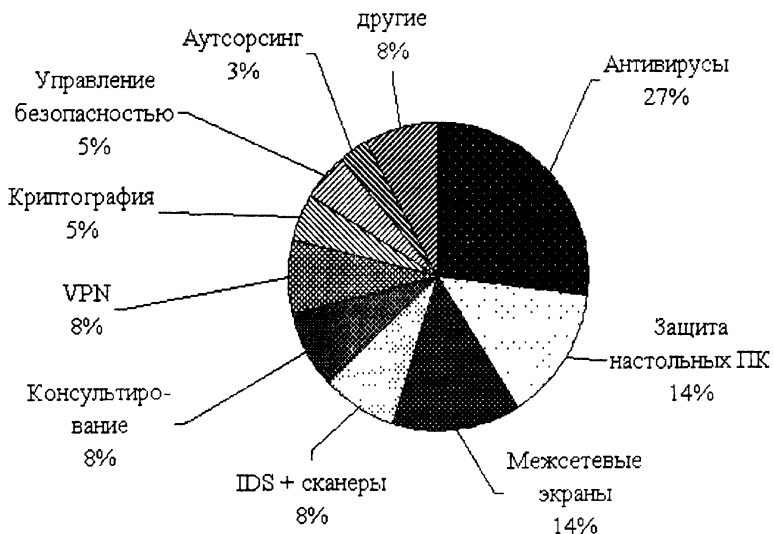


Рис. 2. Соотношение использования средств ИБ в России

Рассмотрение негативных последствий предполагает обязательную идентификацию возможных источников угроз, выявление факторов, способствующих их появлению, и в конечном итоге определение актуальных угроз безопасности информации. Основным критерий для выбора уровня защиты – важность информации.

При разработке общей стратегии организации информационной безопасности (отдельного компьютера, локальной сети, корпоративной сети) на первом этапе должен быть создан документ, в котором будет отражена общая политика безопасности. Определение RFC 2196 описывает политику безопасности следующим образом: "Политика безопасности – это формальное изложение правил, которым должны подчиняться лица, получающие доступ к корпоративной технологии и информации". Можно определить, что *политика безопасности* – это подробный перечень всех требований, которые предъявляются к уровню защиты системы (отдельного компьютера, локальной сети, корпоративной сети). Этот документ должен отражать в себе такие важные аспекты, как:

- определение всех пользователей сети (или на одном компьютере);
- определение прав доступа для всех пользователей. При этом под правами доступа понимается список всех имеющихся ресурсов в системе, с указанием, кто из пользователей имеет к ним доступ. Сам уровень доступа может также существенно варьироваться для различных пользователей и называется правами доступа: право доступа только на чтение, право доступа для чтения и записи, право доступа для переименования объектов, право доступа для удаления объектов, и т.д.

Например, для пользователя с именем Иванов может быть запрещен доступ к принтеру, и данный пользователь не сможет производить распечатку своих материалов на этом принтере. Этому же пользователю можно дать право "только чтение" на все содержимое диска С. Пользователю с именем Петров можно дать полный доступ на диск С (полный доступ означает присутствие всех возможных прав доступа). В результате Иванов сможет только просматривать объекты, расположенные на диске С, но не сможет вносить на него какие-либо изменения (удалять, модифицировать, добавлять объекты), а Петров сможет сделать с диском

С абсолютно все (даже отформатировать его – поэтому не следует давать полный доступ к объекту пользователям, а предоставлять их исключительно администратору).

- определение сетевого программного обеспечения, которое будет использоваться в системе для обеспечения функционирования сети (имеет смысл только в локальных и корпоративных сетях). На этом этапе определяются программные компоненты устанавливаемого сетевого обеспечения. Сюда можно отнести выбор протоколов для передачи информации по сети, выбор сетевой операционной системы. От результатов данного выбора будет зависеть производительность и надежность проектируемой системы.
- определение программного обеспечения, функционирующего в рамках сети. На данном шаге должен быть составлен полный список программного обеспечения, который будет использоваться всеми (или частью) сотрудниками в организации. Возможен запрет на использование какой-либо программой для определенных групп пользователей. Данный список позволит в дальнейшем четко отслеживать "подозрительную" активность некоторых пользователей сети, связанную с неиспользуемыми приложениями и направленную на получение несанкционированного доступа к имеющимся ресурсам.
- определение состава и выработка правил функционирования устройств, обеспечивающих выход в глобальную общедоступную сеть (Интернет). На этом этапе должен быть определен способ подключения к Интернет (по выделенному каналу, по модему или др.), тип маршрутизатора (устройства, обеспечивающего подключение локальной сети к сети Интернет), и должна быть произведена соответствующая настройка этого устройства на выполнение строго определенного рода задач.
- определение порядка протоколирования действий пользователей и записи событий в системный журнал событий. Журнал событий представляет собой электронный аналог обычного журнала, в который могут быть занесены все или часть событий, происходящих в системе. Обычно в такой журнал заносятся системные и сетевые события, выходящие за рамки обычных, например, попытка получения доступа к неразрешенному ресурсу для какого-либо пользователя, попытка открытия файла дан-

ных, к которому нет права на чтение и т.д. Журнал событий должен быть доступен только лицам, отвечающим за функционирование сети. Анализируя записи в этом журнале, администраторы сети могут сделать выводы о степени надежности системы и пресечь попытки на получение несанкционированного доступа к информации.

- определение порядка работы пользователей в сети Интернет. На этом шаге обычно выбирается соответствующее программное или программно-аппаратное обеспечение, которое позволяет вести строгий учет активности всех пользователей в сети Интернет. В частности, здесь могут быть определены список разрешенных для посещения сайтов, время посещения, лимитирован объем передаваемой информации и др.
- определение средств и порядка функционирования средств антивирусной защиты.
- определение средств и порядка функционирования средств обнаружения удаленных атак.

Как можно заметить, политика безопасности затрагивает абсолютно все аспекты функционирования системы и должна иметь комплексный подход к составлению. Нарушение безопасности информации может проявляться по-разному: например, при передаче финансовой бухгалтерской информации от организации в банк (система Клиент–Банк) в виде платежных поручения проблема представляет угроза искажения данных или использование платежных реквизитов – в данном случае необходимо обеспечивать целостность данных при передаче; в сетях же военного ведомства перехват и прочтение передаваемой сверхсекретной информации может стать катастрофой для данного ведомства и в данном случае основным является требование невозможности перехвата информации.

С инструкциями и примерами политики безопасности можно познакомиться на следующих WEB–страницах:

- RFC 2196 "Site Security Handbook" (настольная книга по сетевой безопасности) – <http://www.ietf.org/rfc/rfc2196.txt>;
- пример политики безопасности из университета штата Иллинойс – <http://www.ait.s.uillinois.edu/security/securestandards.html>;

- проектирование и реализация корпоративной политики безопасности – <http://www.knowcisco.com/content/1578700434/ch06.shtml> .

2. Угрозы информационной безопасности.

Всем защитным мерам должен предшествовать анализ угроз. Исследование и анализ многочисленных случаев воздействий на информацию и несанкционированного доступа к ней показывают, что их можно разделить на случайные и преднамеренные.

Информация в процессе ввода, хранения, обработки, ввода и передачи подвергается различным случайным воздействиям.

Причинами таких воздействий могут быть:

- Отказы и сбои аппаратуры (например, отказы источников питания и скачки напряжения).
- Помехи на линии связи от воздействий внешней среды.
- Ошибки человека как звена системы – могут подразделяться на *логические* (неправильно принятые решения), *сенсорные* (неправильное восприятие оператором информации) и *оперативные* или *моторные* (неправильная реализация решения).
- Системные и системотехнические ошибки разработчиков.
- Структурные, алгоритмические и программные ошибки.
- Аварийные ситуации – пожар и природные явления (молния, наводнения, бури и землетрясения).
- Другие воздействия.

Преднамеренные угрозы связаны с действиями человека, причинами которых могут быть определенное недовольство своей жизненной ситуацией, сугубо материальный интерес или простое развлечение с самоутверждением своих способностей, как у хакеров, и т.д. Для вычислительных систем характерны следующие штатные каналы доступа к информации:

- Рабочие места пользователей, администратора системы.
- Средства отображения информации.
- Средства загрузки программного обеспечения.
- Средства документирования информации.

- Носители информации.
- Внешние каналы связи.

Дополнительно доступ к информации может быть получен из-за:

- Побочное электромагнитное излучение аппаратуры системы.
- Побочные наводки по сети электропитания и заземления аппаратуры.
- Побочные наводки на вспомогательных и посторонних коммуникациях.
- Отходы обработки информации в виде бумажных и магнитных носителей.

Угрозами безопасности для информационных ресурсов являются:

- хищение (копирование) информации;
- уничтожение информации;
- модификация (искажение) информации;
- нарушение доступности (блокирование) информации;
- отрицание подлинности информации;
- навязывание ложной информации.

Факторы, влияющие на безопасность информации, можно разделить на следующие группы:

1. Объективные – определяются особенностями построения и техническими характеристиками используемого оборудования:
 - излучения, которые сопутствуют техническим средствам: электромагнитные, электрические и звуковые;
 - активируемые: аппаратные (например, устройства, устанавливаемые на телефонных линиях – "жучки") и программные (например, технологические "дыры" в программном обеспечении) компоненты;
 - определяемые особенностями элементов оборудования: имеющими электроакустические преобразователи (микрофоны, акустические системы) или подверженные воздействию электромагнитного поля (магнитные носители, микросхемы);
 - определяемые особенностями организации работы с оборудованием: его местоположением (например, прямое наблюдение выполняемых на нем действий) и организацией каналов (радио или глобальных сетевых) для обмена информацией.

2. Субъективные – зависят от степени подготовленности и действий (несознательных или целенаправленных) сотрудников:
 - ошибки при работе с программным обеспечением, при управлении сложными системами или при эксплуатации технических средств;
 - нарушения режима охраны и защиты, режима эксплуатации технических средств, режима использования информации, режима конфиденциальности.
3. Случайные – зависят от особенностей окружающей среды и непредвиденных обстоятельств:
 - повреждения жизнеобеспечивающих коммуникаций или ограждающих конструкций;
 - сбои и отказы: отказы и неисправности технических средств, старение и размагничивание носителей информации, сбои программного обеспечения, сбои электроснабжения.

Несмотря на то, что изучение каналов несанкционированного доступа продолжается до сих пор, еще в начале 80-х годов были сформулированы пять основных категорий угроз безопасности данных в вычислительных сетях:

1. Раскрытие содержания передаваемых сообщений.
2. Анализ трафика, позволяющий определить принадлежность отправителя и получателя данных к одной из групп пользователей сети, связанных общей задачей.
3. Изменение потока сообщений, что может привести к нарушению режима работы какого-либо объекта, управляемого из удаленного рабочего места.
4. Неправомерный отказ в предоставлении услуг.
5. Несанкционированное установление соединения.

Угрозы 1 и 2 можно отнести к утечке информации, угрозы 3 и 5 – к ее модификации, а угрозу 4 – к нарушению процесса обмена информацией.

Любая потенциальная угроза связана с определением причиняемого ею ущерба. Проявления возможного ущерба могут быть различны:

- моральный и материальный ущерб деловой репутации организации;

- моральный, физический или материальный ущерб, связанный с разглашением персональных данных отдельных лиц;
- материальный (финансовый) ущерб от разглашения защищаемой (конфиденциальной) информации;
- материальный (финансовый) ущерб от необходимости восстановления нарушенных защищаемых информационных ресурсов;
- материальный ущерб (потери) от невозможности выполнения взятых на себя обязательств перед третьей стороной;
- моральный и материальный ущерб от дезорганизации деятельности организации;
- материальный и моральный ущерб от нарушения международных отношений.

Кратко назовем некоторые из основных существующих методов, предотвращающих катастрофическую потерю данных (более подробное изложение будет дальше):

- резервное копирование;
- источники бесперебойного питания;
- отказоустойчивые системы;
- предупреждение кражи данных;
- пароли и шифрование;
- аудит – это запись определенных событий в журнал безопасности сервера;
- бездисковые компьютеры;
- обучение пользователей;
- физическая защита оборудования;
- защита от вирусов.

3. Средства защиты информации в ЛВС.

Принято различать пять основных средств защиты информации:

- Технические.
- Программные.
- Криптографические.

- Организационные.
- Законодательные.

Рассмотрим эти средства подробнее и оценим их возможности в плане дальнейшего их использования при проектировании конкретных средств защиты информации в ЛВС.

3.1. Технические средства защиты.

Технические средства защиты – это механические, электромеханические, оптические, радио, радиолокационные, электронные и другие устройства и системы, способные выполнять самостоятельно или в комплексе с другими средствами функции защиты данных.

Технические средства защиты делятся на *физические* и *аппаратные*. К физическим средствам относятся замки, решетки, охранные сигнализации, оборудование КПП и др.; к аппаратным – замки, блокировки и системы сигнализации о вскрытии, которые применяются на средствах вычислительной техники и передачи данных.

3.2. Программные средства защиты.

Программные средства защиты – это специальные программы, включаемые в состав программного обеспечения системы, для обеспечения самостоятельно или в комплексе с другими средствами, функций защиты данных.

По функциональному назначению программные средства можно разделить на следующие группы:

1. Программные средства идентификации и аутентификации пользователей.

Идентификация – это присвоение какому-либо объекту или субъекту уникального образа, имени или числа.

Установление подлинности (аутентификация) заключается в проверке, является ли проверяемый объект (субъект) тем, за кого себя выдает.

Конечная цель идентификации и установления подлинности объекта в вычислительной системе – допуск его к информации ограниченного

пользования в случае положительного результата проверки или отказ в допуске в противном случае.

Одним из распространенных методов аутентификации является присвоение лицу уникального имени или числа – пароля и хранение его значения в вычислительной системе. При входе в систему пользователь вводит свой код пароля, вычислительная система сравнивает его значение со значением, хранящимся в своей памяти, и при совпадении кодов открывает доступ к разрешенной функциональной задаче, а при несовпадении – отказывает в нем.

Наиболее высокий уровень безопасности входа в систему достигается разделением кода пароля на две части, одну, запоминаемую пользователем и вводимую вручную, и вторую, размещаемую на специальном носителе – карточке, устанавливаемой пользователем на специальное считывающее устройство, связанное с терминалом.

2. Средства идентификации и установления подлинности технических средств.

Дополнительный уровень защиты по отношению к паролям пользователей.

В ЛВС (у администратора) хранится список паролей и другая информация о пользователях, которым разрешено пользоваться определенными рабочими местами, а также таблица ресурсов, доступных с определенного рабочего места конкретному пользователю.

3. Средства обеспечения защиты файлов.

Вся информация в системе, хранимая в виде файлов делится на некоторое количество категорий по различным признакам, выбор которых зависит от функций, выполняемых системой. Наиболее часто можно встретить разделение информации:

- по степени важности;
- по степени секретности;
- по выполняемым функциям пользователей;
- по наименованию документов;
- по видам документов;

- по видам данных;
- по наименованию томов, файлов, массивов, записей;
- по имени пользователя;
- по функциям обработки информации: чтению, записи, исполнению;
- по областям оперативной и долговременной памяти;
- по времени и т.д.

Доступ должностных лиц к файлам осуществляется в соответствии с их функциональными обязанностями и полномочиями.

4. Средства защиты операционной системы и программ пользователей.

Для защиты пользовательских программ применяется ограничение доступа к занимаемой этими программами памяти.

Защита операционной системы – наиболее приоритетная задача. Осуществляется запретом доступа в области памяти, в которых размещается операционная система.

5. Вспомогательные средства.

К вспомогательным средствам программной защиты информации относятся:

- Программные средства контроля правильности работы пользователей.
- Программные уничтожители остатков информации.
- Программы контроля работы механизма защиты.
- Программы регистрации обращений к системе и выполнения действий с ресурсами.
- Программы формирования и печати грифа секретности.
- Программные средства защиты от компьютерных вирусов и др.

3.3. Криптографические средства защиты.

Криптографические средства защиты – это методы специального шифрования данных (рис. 3), в результате которого их содержание становится недоступным без применения некоторой специальной информации и обратного преобразования.

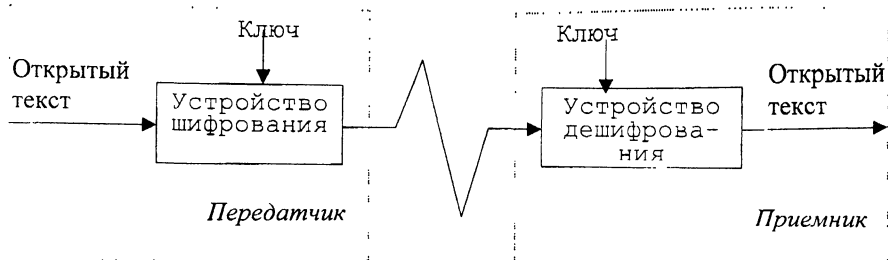


Рис. 3. Шифрование информации

Криптографическая защита (рис. 4) заключается в преобразовании составных частей информации (слов, букв, слогов, цифр) с помощью специальных алгоритмов, либо аппаратных решений и кодов ключей, т.е. приведении ее к неясному виду. Для извлечения закрытой информации применяется обратный процесс – декодирование (дешифрование).

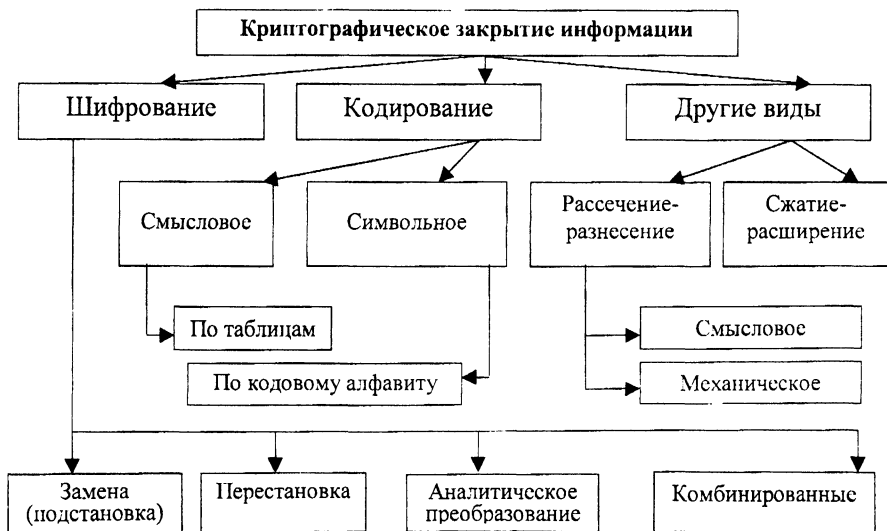


Рис. 4. Классификация методов криптографии

Применение криптографии – один из распространенных методов, значительно повышающих безопасность передачи данных в компьютерных сетях,

данных, хранящихся в удаленных устройствах памяти, и при обмене информацией между удаленными объектами.

3.4. Организационные средства защиты.

Организационные средства защиты – специальные организационно-технические и организационно-правовые мероприятия, акты и правила, осуществляемые в процессе создания и эксплуатации системы для организации и обеспечения защиты информации.

Организационные мероприятия осуществляют двойную функцию:

- Полное или частичное перекрытие каналов утечки информации.
- Объединение всех используемых средств защиты в целостный механизм.

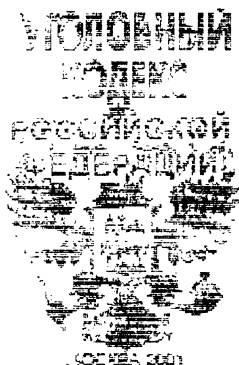
Оргмеры по защите информации должны охватывать этапы проектирования, изготовления, испытаний, подготовки к эксплуатации и эксплуатации системы.

3.5. Законодательные средства защиты.

Законодательные средства защиты – это законодательные акты, которые регламентируют правила использования и обработки информации, и устанавливают ответственность и санкции за нарушение этих правил.

Законодательные меры по защите информации от несанкционированного

доступа заключаются в исполнении существующих в стране или введении новых законов, постановлений, положений и инструкций, регулирующих юридическую ответственность должностных лиц – пользователей и обслуживающего персонала за утечку, потерю или модификацию доверенной ему информации, подлежащей защите, в том числе за попытку преднамеренного несанкционированного доступа к аппаратуре и информации. Таким образом цель законодательных мер – предупреждение и сдерживание потенциальных нарушителей.



4. Права пользователя и защита корпоративной сети.

В общем случае *права пользователя* определяют разрешенные типы действий для этого пользователя. Действия, регулируемые правами, включают вход (регистрацию) в компьютерную сеть и локальное рабочее место (компьютер), использование, установку, копирование, восстановление и удаление файлов и выполнение других задач.

Существуют системы, требующие от пользователя при операциях с зашифрованными файлами и каталогами, а также приложениями (программами) системы использования специальных секретных ключей, записанных на сменных носителях (дискетах, магнитооптических дисках) – ключевых дисках.

Рассмотрим простой пример использования специальных программно-аппаратных средств защиты информации при входе в компьютерную сеть на примере обслуживания пластиковых карт через банкомат Сбербанка.

На рис. 5 показана типичная процедура входа пользователя в систему с применением двойной идентификации (пароль + дополнительное средство проверки полномочий). Число попыток идентификации ограничено: при превышении их количества рабочая станция будет заблокирована. Все действия пользователя регистрируются в системном журнале, содержимое которого может быть в последствии просмотрено и проанализировано. При возникновении события несанкционированного доступа к информации, происходит оповещение администратора безопасности системы, а он уже принимает решение о принятии соответствующих мер. Рассмотрим это подробнее.

4.1. Идентификация пользователя при удаленном обслуживании.

Современные технологии дают пользователям возможность осуществлять оплату товаров и услуг, электронные средства связи позволяют:

- осуществлять электронные платежи и расчеты в точке продажи;
- использовать клиентские терминалы, осуществляющие прямую связь с банком;
- проводить банковское обслуживание с помощью персонального компьютера или телефона;

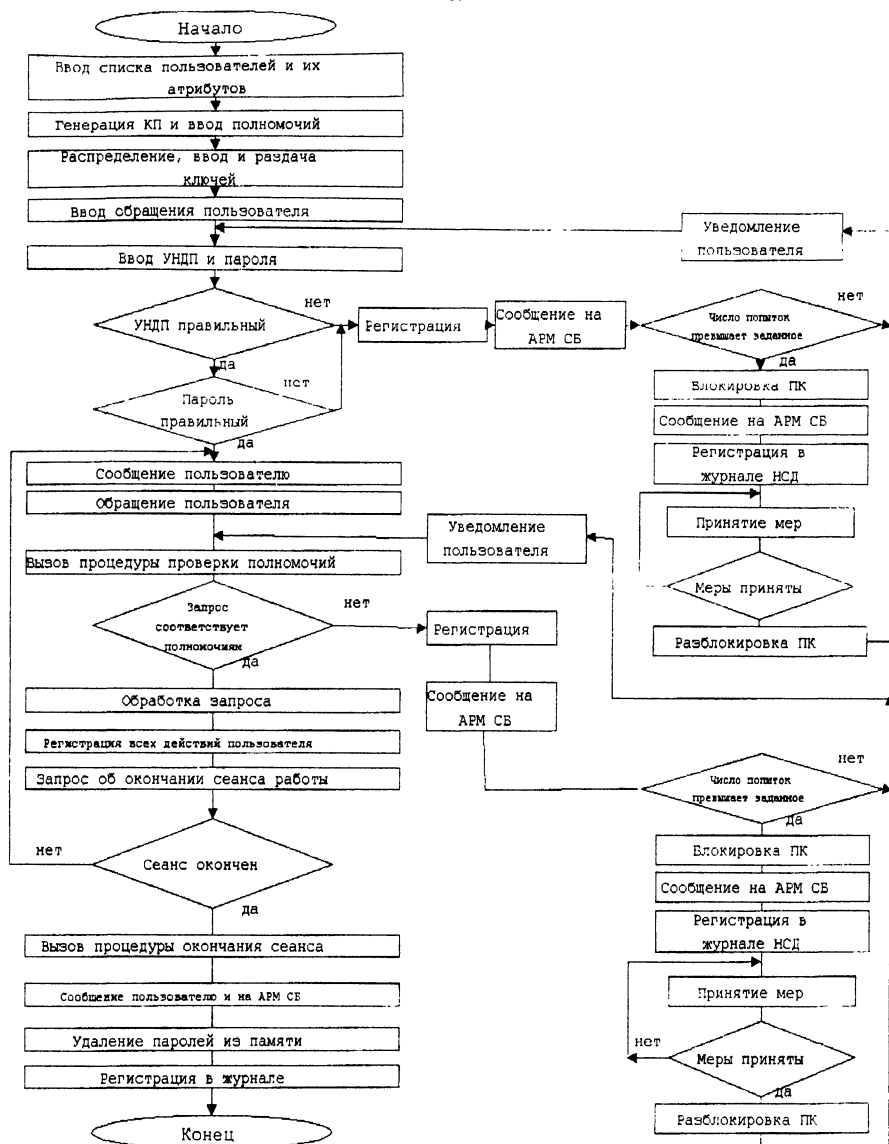


Рис. 5. Схема алгоритма функционирования средств защиты информации:

КП – ключ пользователя

НСД – несанкционированный доступ

УНДП – унифицированная идентификация пользователя

ПК – пластиковая карта

АРМ СБ – автоматизированное рабочее место Сбербанка

- обеспечивать обмен электронными данными в сети с расширенным набором услуг;
- использовать технологии электронных банковских карт, включая магнитные пластиковые и интеллектуальные карты.

Использование систем банкоматов и POS (оплаты покупок и услуг) потребовало появления некоторого носителя информации, который мог бы идентифицировать пользователя и хранить некоторые учетные данные. В качестве такого носителя стали выступать пластиковые карточки. Уже выпущено более миллиарда карточек в различных странах мира. Наиболее известные из них кредитные карточки Visa и MasterCard, карточки для оплаты путешествий и развлечений American Express.

По принципу действия можно выделить пассивные и активные пластиковые карточки. Пассивные всего лишь хранят информацию на том или ином носителе. На магнитной карточке расположена магнитная полоса. Размеры карточки, формат хранимых данных определены специальным стандартом ISO 7811 1985 года. Отличительной особенностью активных карточек является наличие встроенной в него микросхемы. Карточка с микропроцессором называется "интеллектуальной" (smart card). Микросхемы, установленные на карточке, могут быть как обычными – энергонезависимой памяти, так и достаточно сложными микропроцессорами. Емкость обычной карточки с энергонезависимой памятью составляет от 2 до 16 килобайт. В постоянное запоминающее устройство, установленное на карточке, прошивается специальный набор программ. Иначе говоря, сердцем таких карточек является не просто микропроцессор, а микроЭВМ. Эти карточки обеспечивают обширный набор функций:

- возможность работы с защищенной файловой системой (доступ к файлам требует предъявления полномочий по чтению/записи информации);
- шифрование данных с применением различных алгоритмов;
- ведение ключевой системы и т.д.

Некоторые карточки обеспечивают режим "самоблокировки" (невозможность дальнейшей работы с ней) при попытке несанкционированного доступа.

Для обслуживания пластиковой карты через банкомат ее владелец должен знать персональный идентификационный номер–код (ПИН). Для ввода ПИН при использовании банкомата и в терминалах систем POS предусмот-

рена цифровая клавиатура, аналогичная телефонной. Преимуществом интеллектуальных карточек является больший объем хранимой информации, устойчивость к подделке и возможность использования во многих приложениях. Интеллектуальные карточки позволяют существенно упростить процедуру идентификации клиента. Для проверки ПИН применяется алгоритм, реализуемый микропроцессором на карточке.

По способу назначения можно выделить следующие типы ПИН:

- назначаемые выведенные ПИН;
- назначаемые случайные ПИН;
- ПИН, выбираемые пользователем.

Клиент различает только два типа ПИН: ПИН, который назначен ему банком, выдавшим карточку, и ПИН, который пользователь может выбирать себе самостоятельно. В связи с тем, что ПИН предназначен для идентификации и аутентификации клиента, его значение должно быть известно только клиенту.

ПИН обычно состоит из 4–6 цифр. Следовательно, для получения значения 4–х символьного ПИН в наихудшем для защиты случае необходимо осуществить перебор 10 тысяч комбинаций. Такой перебор возможен за короткое время. Поэтому в системах, использующих такой ПИН, должны быть предусмотрены меры защиты от подбора ПИН. Всего существуют два основных способа проверки ПИН: алгоритмический и неалгоритмический.

Алгоритмический способ проверки заключается в том, что у пользователя запрашивается ПИН, который преобразуется по определенному алгоритму с использованием секретного ключа и затем сравнивается со значением ПИН, хранившемся на карточке. Достоинством этого метода проверки является:

- отсутствие копии ПИН на главном компьютере, что исключает его раскрытие персоналом банка;
- отсутствие передачи ПИН между банкоматом и главным компьютером банка, что исключает его перехват злоумышленником или навязывание результатов сравнения;
- облегчение работы по созданию программного обеспечения системы, т.к. уже нет необходимости действий в реальном масштабе времени.

Неалгоритмический способ проверки ПИН, как это следует из его названия, не требует применения специальных алгоритмов. Проверка ПИН осуще-

ствляется путем прямого сравнения полученного ПИН со значениями, хранящимися в базе данных. Часто сама база данных со значениями ПИН шифруется прозрачным образом, чтобы не затруднять процесс сравнения, но повысить ее защищенность.

Для борьбы с подбором ПИН применяется ограничение на его ввод – обычно трехкратное. Если три попытки ввода ПИН оказались неудачными, то в платеже клиенту отказывается.

Кроме одиночных банкоматов в настоящее время эксплуатируются и сети банкоматов, в которых участвуют несколько банков. При совместном использовании банками сети банкоматов появляется новая проблема – защита конфиденциальной информации банков друг от друга (ключи шифрования, списки номеров запрещенных к использованию карточек и т.д.). Для ее успешного решения была предложена схема централизованной проверки ПИН каждым банком в своем центре связи с банкоматом. При этом также усложняется система распределения ключей между всеми участниками сети. Наиболее часто используется следующий метод: вся сеть банкоматов разбита на зоны и в каждой из них используется свой Главный зональный управляющий ключ. Он предназначен для шифрования ключей при обмене между сетевым маршрутизатором и главным компьютером банка. Ключ индивидуален для всех участников сети. Обычно он случайно генерируется маршрутизатором и незлектронным способом передается в банк. Раскрытие ключа приведет к раскрытию всех ПИН, которые передаются между маршрутизатором и главным компьютером банка.

4.2. Механизмы защиты информации в корпоративной сети.

1. Аутентификация пользователей при подключении к сети:

при регистрации на сервер передается идентификатор, введенный пользователем (рис. 6). По этому идентификатору ОС NetWare выполняет поиск соответствующего объекта пользователя в системной базе данных сетевых ресурсов.

Если в базе данных хранится значение пароля для этого клиента, то ОС NetWare посылает на рабочую станцию зашифрованный с помощью пароля открытый ключ (симметричное шифрование). На рабочей станции этот

ключ расшифровывается с помощью пароля, введённого пользователем, и используется для получения подписи запроса (пакета) к серверу о продолжении работы. Сервер расшифровывает эту подпись с помощью закрытого ключа (асимметричное шифрование), проверяет её и посылает подтверждение на рабочую станцию. В дальнейшем каждый NCP-пакет снабжается подписью, получаемой в результате кодирования открытым ключом контрольной суммы содержимого пакета и случайного числа Nonce. Это число генерируется для каждого сеанса. Поэтому подписи пакетов не повторяются для разных сеансов, даже если пользователь выполняет те же самые действия.

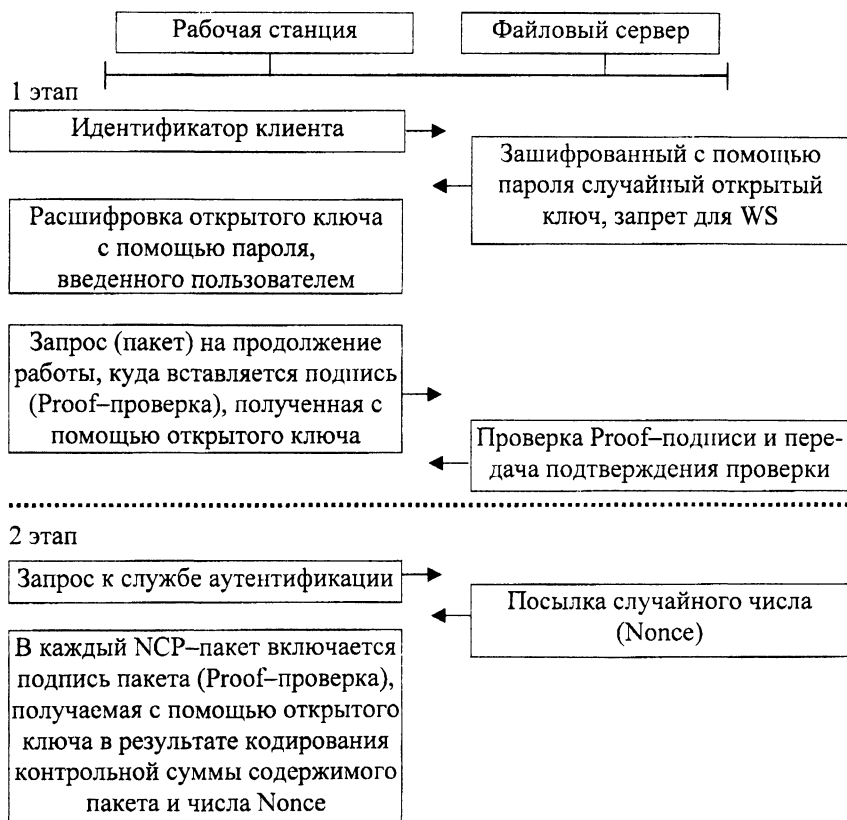


Рис. 6. Аутентификация клиента

2. Авторизация доступа к данным сети:

в ОС NetWare реализованы три уровня защиты данных (рис. 7).

Здесь под аутентификацией понимается:

процесс подтверждения подлинности клиента при его подключении к сети, процесс установления подлинности пакетов, передаваемых между сервером и рабочей станцией.

Права по отношению к файлу (каталогу) определяют, какие операции пользователь может выполнить с файлом (каталогом). Администратор может для каждого клиента сети определить права по отношению к любому сетевому файлу или каталогу. Атрибуты определяют некоторые системные свойства файлов (каталогов). Они могут быть назначены администратором для любого сетевого файла или каталога. Следует отметить, что атрибуты файла (каталога) имеют более высокий приоритет, чем права пользователей по отношению к этому файлу.

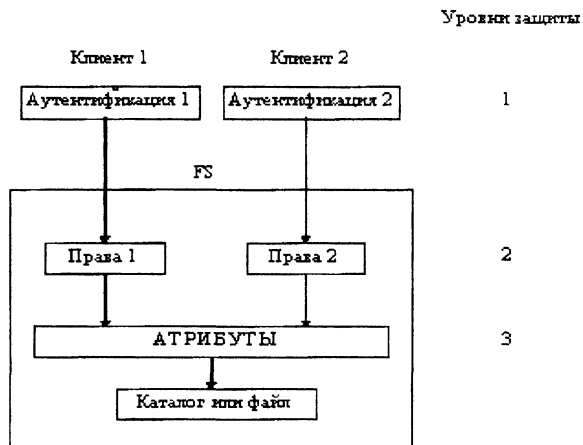


Рис. 7. Уровни защиты информации в ОС NetWare

Например, чтобы записать данные в файл, клиент должен:

- знать свой идентификатор и пароль для подключения к сети,
- иметь право записи данных в этот файл,
- файл должен иметь атрибут, разрешающий запись данных.

5. Безопасность корпоративной сети при выходе в Интернет.

Термин безопасность в Интернет звучит как сочетание несовместимых понятий. Назначение Интернет – обеспечение открытой коммуникационной платформы между пользователями. Модель универсального неограниченного доступа вначале устраивала многих пользователей. Однако необходимость выхода в Интернет организаций, имеющие свои секреты (государственные и оборонные учреждения, коммерческие фирмы и пр.), и быстрое начало коммерциализации Интернета (например, введение кредитных карточек, e-бизнес) привело к необходимости конфиденциальности при размещении информации в Интернете. Рост "киберпреступности" требует от пользователей защищать свою информацию. Много организаций было атаковано или зондировано злоумышленниками, в результате чего они понесли большие финансовые потери и утратили свой престиж. В некоторых случаях организации были вынуждены временно отключиться от Интернета и потратили значительные средства на устранение проблем с конфигурациями серверов и сетей. Узлы, которые неосведомлены или игнорируют эти проблемы, подвергают себя риску сетевой атаки злоумышленниками. Даже те сайты, которые внедрили у себя меры по обеспечению безопасности, подвергаются тем же опасностям из-за появления новых уязвимых мест в сетевых программах и настойчивости некоторых злоумышленников.

Безопасность при использовании Интернет представляет интерес для 2-х категорий людей – тех, кто должен защищать информацию, и тех, кто намеревается получить к ней доступ. Специфика заключается в том, что больше достоверной информации об обеспечении безопасности могут получить у хакеров (если они захотят ею поделиться), а не у профессионалов, которые предпочитают не раскрывать своих секретов.

Фундаментальная проблема состоит в том, что Интернет при проектировании и не задумывался как защищенная сеть. Интернет создавался для связи между государственными учреждениями и университетами в помощь учебному процессу и научным исследованиям. Никто не предполагал, что эта глобальная сеть получит более широкое применение. Поэтому спецификации первых версий Интернет-протокола IP не содержали требования по обеспечению безопасности, а в итоге многие реализации IP оказались по-существу уязвимыми. После возникновения проблем появилась необходимость вне-

дрения средств безопасности для IP. Но из-за первоначального отсутствия при создании протокола IP средств защиты пришлось все его реализации просто дополнять разнообразными сетевыми процедурами, услугами и программным обеспечением, уменьшающими риски, присущие этому протоколу. Существуют определенные проблемы в используемых протоколах:

- Легкость перехвата данных и фальсификации адресов машин в сети – основная часть трафика Интернета – это нешифрованные данные. E-mail, пароли и файлы могут быть перехвачены, используя легко доступные программы.
- Уязвимость средств TCP/IP – ряд средств TCP/IP не проектировался с элементами защиты и может быть скомпрометирован квалифицированными злоумышленниками; средства, используемые для тестирования особенно уязвимы.
- Отсутствие политики – многие узлы по незнанию сконфигурированы таким образом, что предоставляют широкий доступ к себе со стороны Интернета, не учитывая возможность злоупотребления этим доступом; многие узлы разрешают работу большего числа сервисов TCP/IP, чем им требуется для работы и не пытаются ограничить доступ к информации о своих компьютерах, которая может помочь злоумышленникам.
- Сложность конфигурирования – средства управления доступом сервера сложны; зачастую сложно правильно сконфигурировать и проверить эффективность установок. Средства, которые по ошибке неправильно сконфигурированы, могут привести к неразрешенному доступу.

5.1. Мероприятия по обеспечению безопасности.

Для обеспечения безопасности корпоративной сети при выходе в Интернет используются упоминавшиеся ранее средства и мероприятия по защите – технические, программные, криптографические, организационные и законодательные.

К передачи информации по общедоступным глобальным каналам в настоящее время предъявляются следующие основные требования:

- целостность информации, под этим термином понимается наличие сто-процентной уверенности в том, что информация, посланная отправите-

лем, в точности соответствует информации, прибывшей к получателю, т.е., что информация дошла до получателя без искажений;

- подлинность отправителя – гарантирует, что отправитель в последствии не сможет отказаться от факта отправки какой-либо информации в сеть;
- невозможность прочтения при перехвате – гарантирует, что даже если в процессе передачи информации по каналам глобальной сети, злоумышленнику удалось перехватить информацию, он не сможет ее прочесть в исходном виде. Основным способом, обеспечивающим данную возможность, является применение сложных механизмов шифрования данных;
- невозможность искажения информации – предусматривает, что отправитель однозначно может определить, что дошедшая до него информация изменена или модифицирована, и проинформировать об этом отправителя.

Соблюдение всех этих требований позволяет создать по-настоящему безопасную систему, удовлетворяющую современным требованиям. К числу средств, обеспечивающих покрытие некоторых или сразу всех вышеперечисленных требований, можно отнести:

1. Использование аппаратных или программно-аппаратных средств шифрования (криптографических) исходящего трафика сети. В основе любой системы криптографии находятся две составляющие: алгоритм шифрования и ключ шифрования. Алгоритм шифрования определяет каким образом исходные, незашифрованные данные (в литературе встречается понятие "чистые данные") будут преобразовываться в секретную кодировку, а ключ определяет то секретное слово или фразу, с помощью которого алгоритм будет выполняться. В настоящее время применяют достаточно сложные алгоритмы шифрования с длиной ключа 128 или 256 бит. Распространенными примерами криптографических алгоритмов являются системы DES, RSA.
2. Использование программно-аппаратных анализаторов сетевого трафика. Данный класс устройств используется для определения характеристик проходящего через него трафика, таких как пропускная способность канала, определение числа "бракованных пакетов" и др. Кроме того, анализаторы в некоторых случаях могут отслеживать "подозрительную" активность в сети.

3. Использование средств цифровой подписи. В рамках данного метода отправитель формирует некоторое сравнительно небольшое слово, правило образования которого однозначно определяется исходным сообщением, и называемое дайджестом. Один дайджест может быть получен только на основе одного сообщения. Адресат сообщения формирует точно такой же дайджест на основе полученного сообщения. Совпадение дайджеста отправителя и получателя гарантирует, что исходное сообщение достигло получателя без искажения, т.е. гарантирует целостность пересылки. Кроме этого, методы цифровой подписи позволяют однозначно определять отправителя сообщения.
4. Использование межсетевых экранов. Именно данная методика является на сегодняшний день наиболее комплексным средством для обеспечения сетевой безопасности. Привлекательность ее состоит и в том, что она может с успехом применяться как на уровне отдельно взятого компьютера, так и в рамках локальной или глобальной сетей.

5.2. Межсетевой экран.

Межсетевой экран (в литературе можно встретить названия *брандмауэр*, *firewall* (англ.)) – представляет собой программно-аппаратное или чисто программное средство, через который проходит весь входящий и исходящий трафик системы. Обычно межсетевой экран ставится на границе локальной сети, непосредственно перед выходом в глобальную сеть.

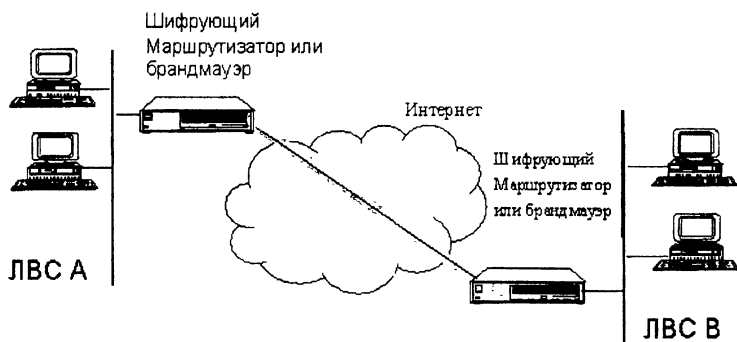


Рис. 8. Соединение 2-х ЛВС через Интернет

Тривиальным случаем брандмауэра является маршрутизатор, который может выступать в роли устройства для фильтрации пакетов (рис. 8).

На рис. 9 показана типичная сетевая архитектура в организации при использовании Интернета.

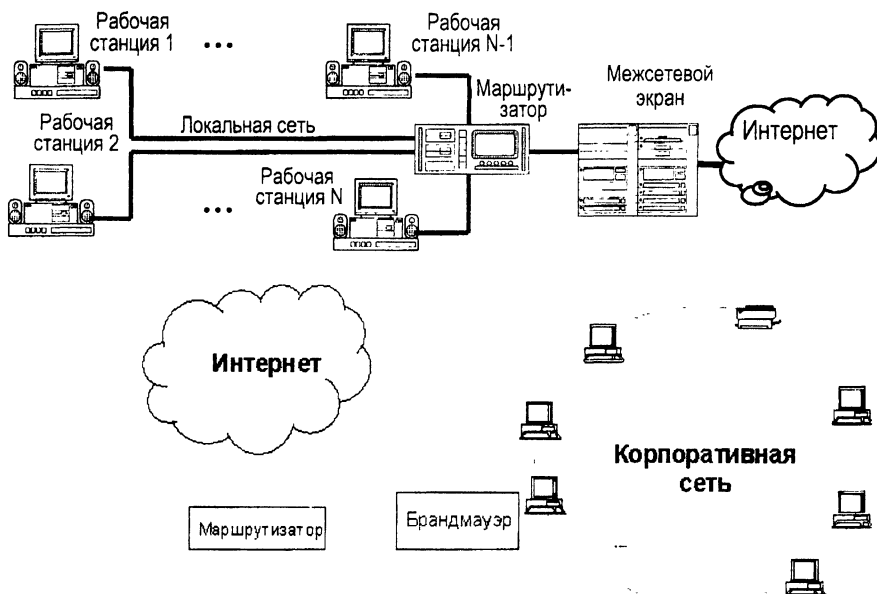


Рис. 9. Типичная архитектура подключения к Интернету

Брандмауэр – это не одна компонента (аппаратная или программная), а стратегия защиты ресурсов организации, доступных из Интернета. Брандмауэр выполняет роль стражи между небезопасным Интернетом и более надежными внутренними (корпоративными) сетями.

Брандмауэры обеспечивают несколько типов защиты и могут:

- блокировать нежелательный трафик;
- направлять входной трафик только к надежным внутренним системам;
- скрыть уязвимые системы, которые нельзя обезопасить от атак из Интернета другим способом;
- протоколировать трафик в и из внутренней сети;

- скрывать информацию, такую как имена систем, топологию сети, типы сетевых устройств и внутренние идентификаторы пользователей, от Интернета;
- обеспечить более надежную аутентификацию, чем та, которую представляют стандартные приложения.

На брандмауэре-компьютере могут быть вызваны специальные программы (называемые прокси-серверами). Эти прокси-сервера принимают запросы извне, анализируют их и передают безопасные запросы внутренним серверам, которые предоставляют соответствующие сервисы. В этом случае могут быть обеспечены такие функции, как аутентификация пользователей и протоколирование их действий.

Принцип работы межсетевого экрана заключается в фильтрации всего трафика сети. Межсетевой экран просматривает все исходящие и входящие пакеты на предмет анализа содержащейся в них информации. Анализ заключается в сопоставлении служебной информации, содержащейся в каждом пакете с набором predetermined на этапе настройки межсетевого экрана правил, регулирующих доступ из/в сеть. Примерами таких правил могут служить:

- ограничение на адреса отправителя или получателя пакета. Возможно задание некоторой группы сетевых адресов, с которых прием пакетов будет запрещен;
- ограничение по размеру передаваемых пакетов. Возможно задание некоторого лимита по количеству байт, содержащихся в каждом пакете;
- и т.д.

Современные модели межсетевых экранов позволяют очень гибко настраивать все правила с точностью до малейших нюансов. Настройка межсетевого экрана должна производиться системным администратором сети, разбирающимся во всех тонкостях функционирования сетевых компонентов.

Межсетевые экраны, работающие по такому принципу, получили название пакетных фильтров, т.к. они просматривают и проверяют все проходящие в сети пакеты. Анализируя служебную информацию в каждом пакете, межсетевой экран принимает по каждому пакету решение. В качестве решений всегда выступают следующие:

pass (пропустить) – пакету разрешается прохождение в сеть;

fail (запретить) – пакет считается опасным и не проходит далее в сеть;
 continue (продолжить) – текущий фильтр не может принять никакого решения по данному пакету, и пакет перенаправляется на обработку последующих фильтров;

drop (отбросить) – пакет отбрасывается (не пропускается), но причина кроется не в “опасности” данного пакета, а в некоторых специфических причинах, например, нет смысла передавать пакет через межсетевой экран, если источник и приемник находятся в одной сети;

error (ошибка) – при обработке пакета произошла некоторая ошибка, она записывается в системный журнал ошибок.

Однако такие брандмауэры не учитывают некоторых особенностей межсетевого взаимодействия, в частности, они проверяют только служебную информацию в пакете и не проверяют самих данных в пакете. Для преодоления этого недостатка был создан новый тип межсетевых экранов, получивший название посредника уровня приложения. Основными функциями данного вида межсетевых экранов является определение конкретного приложения, которому предназначен пакет и запуска соответствующего модуля, который отвечает за это приложение. В итоге получается более гибкая и адаптивная система, позволяющая произвести анализ содержимого пакета и выявить “подозрительные” и “опасные” пакеты. В настоящее время наибольшее применение находят межсетевые экраны, в которых сочетаются два описанных выше метода.

На рис. 10 представлены доли поставщиков на мировом рынке межсетевых экранов (2-й квартал 2001г.) по данным Infonetics Research на август 2001 г., основанным на доходах компаний в размере \$430.7 млн. от мировых продаж.

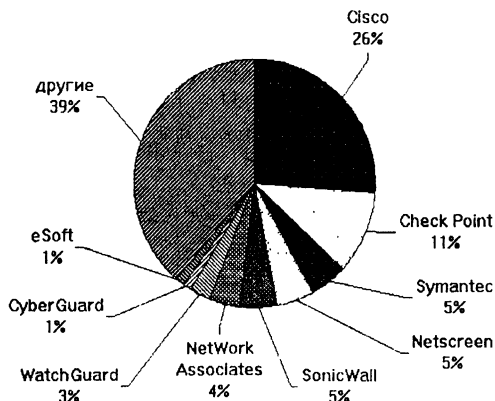


Рис. 10. Соотношение поставщиков межсетевых фильтров

Остановимся на еще одном интересном применении межсетевых экранов – организации виртуальных частных сетей (Virtual Private Network – VPN). Все современные модели межсетевых экранов обязательно должны поддерживать данную возможность. По мере развития телекоммуникационных средств связи и информационных технологий (в том числе средств защиты информации) виртуальные частные сети приобретают все большую привлекательность в качестве инструмента для организации электронного бизнеса, документооборота, оперативного средства совершения финансовых операций и др.

Под термином виртуальной частной сети понимается сеть, обеспечивающая достаточно экономичный, надежный и безопасный способ конфиденциальной связи между бизнес-партнерами, компаниями и их клиентами, отдельными подразделениями предприятия, удаленными сотрудниками и центральным офисом, и все это – на базе сетей общего пользования (Интернет).

В общем случае VPN – это объединение локальных сетей или отдельных машин, подключенных к сети общего пользования, в единую виртуальную (наложенную) сеть, обеспечивающую секретность и целостность передаваемой по ней информации, причем абсолютно прозрачно для пользователей.

Использование технологии VPN необходимо там, где требуется защита корпоративной сети от воздействия вирусов, злоумышленников, просто любопытных, а также от других угроз, являющихся результатом ошибок в конфигурировании или администрировании сети.

Еще совсем недавно считалось, что достаточно высокий уровень информационной безопасности могут обеспечить только корпоративные сети, надежно изолированные от сетей общего пользования за счет прокладки частных выделенных каналов связи и использования собственного коммуникационного оборудования. Однако такой подход к построению защищенных сетей крайне неэкономичен, сами сети плохо масштабируемы, а их кажущаяся изолированность все равно не обеспечивает 100% безопасности информационным потокам. Кроме того, из-за достаточно высоких инсталляционных и эксплуатационных расходов построение разветвленных корпоративных сетей с широким географическим охватом под силу только очень крупным корпорациям и организациям, что уже отмечалось выше.

Виртуальные частные сети VPN, создаваемые на базе арендуемых и коммутируемых каналов связи сетей общего пользования (и, в первую очередь, Интернет), являются отличной альтернативой изолированным корпоративным сетям, причем, альтернативой, обладающей рядом несомненных преимуществ:

- независимость от криптографии. Возможность подключения модулей криптографии от третьих производителей, что позволяет их использовать в любой стране мира в соответствии с принятыми национальными стандартами;
- масштабируемость продуктов позволяет подбирать оптимальное по стоимости и надежности решение с возможностью постепенного наращивания мощности системы защиты;
- наличие открытых интерфейсов для интеграции с другими программными системами и бизнес-приложениями;
- гибкость установки и настройки позволяет внедрить систему безопасности, не меняя сетевой конфигурации корпоративной сети;
- экономичность. При использовании VPN-продуктов не требуются специальные каналы для передачи конфиденциальной информации: защита позволяет передавать конфиденциальную информацию по любым каналам, поддерживающим открытые протоколы;
- поддержка международных стандартов. Совместимость продуктов с продуктами известных производителей.
- высокая надежность;
- легкость изменения конфигурации;
- контроль за событиями и действиями пользователей.

Следует, однако, иметь ввиду, что организация сетей VPN, решая одну проблему – существенное сокращение расходов на поддержание собственных коммуникационных магистралей, тут же на первое место выдвигает другую – обеспечение безопасности, которая при использовании VPN приобретает первостепенное значение.

Какими свойствами должна обладать VPN? Можно выделить три фундаментальных свойства, превращающих наложенную корпоративную сеть, построенную на базе сети общего пользования, в виртуальную частную сеть:

- шифрование,
- аутентификация,
- контроль доступа.

Только реализация всех этих трех свойств позволяет защитить пользовательские машины, серверы предприятия и данные, передаваемые по физически незащищенным каналам связи, от внешних нежелательных вторжений, утечки информации и несанкционированных действий.

Доли поставщиков VPN по данным Infonetics Research на август 2001 г. на мировом рынке (2-й квартал 2001 г.) представлены на рис. 11. Доли поставщиков представлены по доходам, а доля Cisco включает доходы от продажи маршрутизаторов, выполняющих функции VPN. Общий объем мирового рынка во 2-м квартале 2001 г. составил 1.6 млрд. долларов.

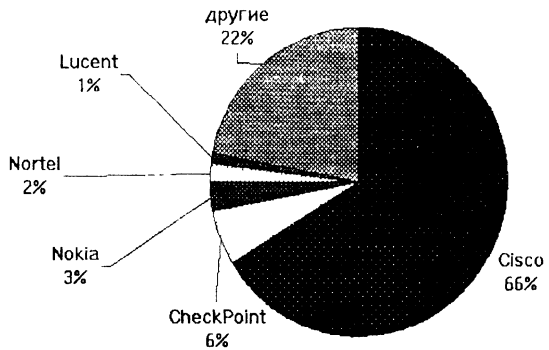


Рис. 11. Соотношение поставщиков VPN

Общий объем мирового рынка во 2-м квартале 2001 г. составил 1.6 млрд. долларов.

5.3. Виды удаленных атак.

В связи с увеличением случаев получения несанкционированного доступа к информации, в основе которых лежит удаленный доступ, т.е. доступ, использующий общедоступные каналы связи (типа Интернет), в задачи межсетевых экранов ставится и обеспечение защиты от такого рода удаленных атак. Под *удаленной атакой* понимается действие одиночного пользователя или группы пользователей сети Интернет, направленное на причинение ущерба другому пользователю или группе пользователей сети Интернет, осуществляемое по общедоступным глобальным каналам связи. Вместе с огромным ростом популярности технологий Интернет возникает беспрецедентная угроза разглашения личных данных, критически важных корпоративных ресурсов, государственных тайн и т.д.

В настоящий момент времени существуют несколько способов осуществления удаленных атак, однако можно выделить следующие основные причины, по которым атаки могут быть успешными:

1. К Интернету уже подключены миллионы устройств и количество подключаемых устройств постоянно возрастает. В итоге вероятность доступа хакеров к уязвимым устройствам увеличивается. Кроме того, предоставляемые Интернетом возможности позволяют хакерам незамедлительно обмениваться информацией в глобальном масштабе, передавать вредоносные коды и способы их использования.
2. Использование ошибок или недоработок в существующих реализациях сетевых компонентов: протоколов, операционных систем и др.
3. Использование ошибок в программном обеспечении, установленном на компьютере (системе) "жертвы".
4. Использование "зомбированных" компьютеров, когда злоумышленник предварительно тем или иным способом устанавливает на компьютере-жертве программное обеспечение, с помощью которого в дальнейшем он может осуществить свою атаку.

Учитывая выше сказанное, следует сразу отметить, что одним из способов повышения уровня безопасности сети является своевременное обновление всего установленного ПО, установка "upgrade'ов" и "hotfix'ов". Это дает гарантию того, что потенциальный злоумышленник не сможет воспользоваться "брешью" в программном обеспечении, установленном на вашем компьютере.

Первые атаки появились сравнительно давно (в 80-е годы), а на сегодняшний день их количество и разнообразие стремительно возрастают. Получили распространение так называемые распределенные атаки, в которых источником атаки является сразу несколько сетевых узлов, которые могут находиться на огромном расстоянии друг от друга. Факт распределенности атаки значительно затрудняет выявление и устранение атак.

Анализируя основные принципы реализации атак, можно выявить следующие их основные типы. Наибольшее распространение получили атаки, получившие название "отказ в обслуживании" ("denial of service", DoS). Данный тип атак направлен на выведение того или иного узла сети из строя. В

ходе атак DoS могут использоваться обычные Интернет-протоколы, такие как TCP и ICMP (Internet Control Message Protocol). Большинство атак DoS опирается не на программные ошибки или бреши в системе безопасности, а на общие слабости системной архитектуры. Обычно выведение из строя ограничивается неспособностью узла обслуживать поступающие на него запросы, хотя некоторые из них могут заставить узлы полностью "зависнуть" и не реагировать даже на локальные запросы. Наибольшую опасность представляют распределенные атаки "отказ в обслуживании", в которых воздействие идет сразу от многих сетевых узлов. Когда атака проводится одновременно через множество устройств, то выполняется распределенная атака DoS (DDoS – distributed DoS). Особую опасность такие атаки представляют для глобальных сетевых порталов (представляющих сетевые услуги для огромного числа пользователей). В качестве примера реализации такого рода атак предлагается рассмотреть сравнительно недавно произошедшие случаи со всемирно-известными порталами Yahoo, CNN и eBay.

Факты гласят, что 7 февраля 2000 года, в 10.20 утра по Тихоокеанскому времени пользователи портала Yahoo (www.yahoo.com) заметили существенное замедление в предоставляемых услугах – электронной почте, новостях и т.д. Пользователи, привыкшие к тому, что среднее время загрузки одной Web-страницы составляло не более 1.7 секунд были раздражены шестисекундными задержками. Дальше стало еще хуже. В 10.30 утра уже половина всех пользователей, пытавшихся получить доступ к серверу Yahoo в ответ получало только сообщение об ошибке. Анализ проблемы показал, что отказ серверов Yahoo был вызван огромным числом небольших пакетов, которые изменялись от простых диагностических сообщений до запросов о получении HTML-страниц. Лавина этих пакетов обрушилась на Yahoo сразу из нескольких точек Интернет. Специалисты Yahoo насчитали не менее 50 таких точек. В 11.00 утра менее 10 процентов всех пользователей Yahoo смогли получить доступ к ресурсам этого портала. И даже тем, кому все-таки удалось "достучаться" до сервера, приходилось ждать не менее 20 секунд пока придет ответ на сделанный запрос. В 13.15 все запросы пользователей были направлены на неатакованные сервера и в 15.00 функционирование Yahoo вернулось в нормальное русло.

Yahoo был первым из серии широко известных серверов, которые подверглись массированным атакам во вторую неделю февраля 2000 года. Сле-

дующими жертвами стали сервера Buy.com, eBay, CNN.com, Amazon.com, ZDNet.com, E*Trade, Datek, Excite. Время, в течение которого данные сервера были недоступны для пользователей, колебалось от 30 минут до нескольких часов.

Второй жертвой стал сервер Buy.com, который подвергся атаке в 10.50, во вторник. Шторм пакетов, направленный на этот узел в 8 раз превысил допустимый объем трафика и достиг отметки в 800 Мбит/сек. Аналогичные результаты наблюдались и у других компаний. Все это стало возможным благодаря распределенным атакам типа "отказ в обслуживании" (Distributed Denial of Service Attacks). Впервые о них заговорили еще в 1998 году, когда Naval Surface Warfare Center (США) опубликовал отчет, посвященный анализу нескольких случаев применения распределенных атак. Второй раз пристальное внимание к распределенным атакам было уделено в конце 1999 года. Было опубликовано несколько документов и предупреждений, в которых говорилось, что опасность применения таких атак очень велика. Однако практически никто не прислушался к этим заявлениям и в начале февраля 2000 года грянул гром. Десятки компаний подверглись распределенным атакам, в т.ч. зафиксированы атаки и на российские компании, использующие Интернет в своей работе. Детально, но не вдаваясь в технические подробности, предлагается рассмотреть технологию реализации таких атак для более осмысленного понимания сути данной проблемы.

Все они основаны на "классических" атаках типа "отказ в обслуживании", точнее на их подмножестве, известном как Flood- или Storm-атаки (указанные термины можно перевести как "шторм", "наводнение" или "лавина"). Смысл данных атак заключается в отправке большого количества пакетов на заданный узел сети (цель атаки), что может привести к выведению этого узла из строя, поскольку он "захлебнется" в лавине посылаемых пакетов и не сможет обрабатывать запросы авторизованных пользователей. По такому принципу работают атаки SYN-Flood, Smurf, UDP Flood, Targa3 и т.д. Однако в том случае, если пропускная способность канала до цели атаки превышает пропускную способность атакующего или целевой узел некорректно сконфигурирован, то к "успеху" такая атака не приведет. В случае же распределенной атаки ситуация коренным образом меняется. Атака происходит уже не из одной точки Интернет, а сразу из нескольких, что приводит к резкому возрастанию трафика и выведению атакуемого узла из строя.

Реализуется распределенная атака в два этапа. Первый этап заключается в поиске в Интернет узлов, которые можно было бы задействовать для реализации распределенной атаки. Чем больше будет найдено таких узлов, тем эффективнее будет атака. "Изюминка" в том, что в Интернет таких узлов миллионы. Проводимые регулярно исследования показывают, что многие компании не следят за безопасностью своих узлов, имеющих выход в Интернет. Эти-то узлы и становятся излюбленным местом злоумышленников, выбирающих их в качестве "базового лагеря" для дальнейшей атаки. Эти узлы могут относиться не только к сетям университетов и государственных структур, как это было в случае с февральскими атаками, но и Интернет-провайдерам, финансовым и страховым компаниям и т.д. После нахождения уязвимых узлов, злоумышленник осуществляет установку на них компонентов, реализующих атаку. Такая установка становится возможной благодаря "слабым" местам, которые и использует злоумышленник для своих "черных дел".

Второй этап заключается в посылке большого числа пакетов на атакуемый узел. Особенность этого этапа в том, что посылка пакетов осуществляется не с узла, за которым непосредственно сидит злоумышленник, а со скомпрометированной им системы, на которой установлены специальные агенты, реализующие распределенную атаку. Существует два типа таких агентов: "мастера" и "демоны" (или "клиенты" и "сервера"). Иногда компьютеры с установленными агентами называют компьютеры-"зомби". Злоумышленник управляет небольшим числом "мастеров", которые в свою очередь командуют "демонами". Вместо обычной одноуровневой структуры обычной атаки (злоумышленник → атакуемый) используется трехуровневая структура (злоумышленник → мастер → демон → атакуемый). Что мешает пройти по этой цепочке и определить все участвующие в атаке узлы? Но в том-то и состоит особенность распределенных атак, что так просто этого не сделать.

Обнаружение и блокирование одного или нескольких "мастеров" или "демонов" не приводит к окончанию действия атаки, поскольку каждый "демон" действует независимо от других и, получив соответствующие команды от "мастера", уже не нуждается в дальнейшем поддержании связи с ним. Т.е. "демон" работает автономно, что существенно затрудняет обнаружение и блокирование всех демонов, участвующих в распределенной атаке. Кроме того, при атаке возможна подмена адреса отправителя враждебных пакетов, что также отрицательно сказывается на эффективности контрмер. Злоумыш-

ленник использует десятки и сотни незащищенных узлов для координации нападения. Эти узлы могут принадлежать различным провайдерам и находиться в различных странах и даже на различных материках, что существенно затрудняет обнаружение злоумышленника, координирующего атаку. Каждый узел, участвующей в скоординированной атаке, не позволяет получить информацию о том, кто и откуда инициировал нападение. Кроме того, на этих узлах нет полного списка, участвующих в атаке узлов. Поэтому выявление одного узла не приводит к предотвращению всей атаки. Этот тип атак трудно предотвратить, т.к. для этого требуется координация действий с провайдером. Если трафик, предназначенный для переполнения вашей сети, не остановить у провайдера, то на входе в сеть это сделать уже невозможно, потому что вся полоса пропускания будет занята.

Приведенные примеры позволяют сделать заключение об опасности такого рода атак. Для организации DoS требуется небольшой объем знаний и умений, но простота реализации и огромный причиняемый вред должны привлекать к DoS особенно пристальное внимание администраторов, отвечающих за сетевую безопасность. Наиболее известные разновидности атак DoS: TCP SYN Flood, Ping of Death, Tribe Flood Network (TFN) и Tribe Flood Network 2000 (TFN2K), Trinco, Stacheldracht, Trinity.

Угроза атак типа DoS может снижаться следующими способами:

- использование функции анти-DoS: правильная конфигурация функций анти-DoS на маршрутизаторах и межсетевых экранах может ограничить эффективность атак. Эти функции часто ограничивают число полуоткрытых каналов в любой момент времени.
- ограничение объема трафика (traffic rate limiting): можно обратиться к провайдеру с просьбой ограничить объем трафика. Этот тип фильтрации позволяет ограничить объем не критического трафика, проходящего по сети. Например, атаки (D)DoS часто происходят через ICMP, который используется для диагностических целей и возможно ограничение объема его трафика.

Следующий тип атаки основан на искажении служебной информации в пакете. Обычно замаскируется исходный адрес отправителя. При этом ситуация обычно выглядит так: злоумышленнику требуется получить несанкционированный доступ к ресурсам какого-либо узла сети. При этом дос-

туп данного пользователя к ресурсам этой сети запрещен (его адрес не пропускает система защиты). Злоумышленник на первом этапе пытается перехватить пакеты пользователей, имеющих доступ к требуемым ресурсам, и расшифровать содержащийся в них адрес отправителя. После этого, на втором этапе, злоумышленник заменяет в своих пакетах свой истинный адрес на адрес, полученный из пакетов авторизованных пользователей. В итоге система-получатель анализирует пришедшие к ней пакеты, определяет, что они пришли от авторизованного пользователя, и в конечном итоге, разрешает доступ злоумышленника к ресурсам сети. Конечно, данный метод требует большей специализированной подготовки злоумышленника, но и он в настоящее время находит широкое применение. Самым важным пунктом при реализации таких атак становится вопрос перехвата передаваемой по сети информации. И опять в этом случае может помочь шифрование трафика – перехватив сообщение, злоумышленник не сможет его прочесть.

Следующий тип атак основан на снифферах пакетов, представляющих собой приложения, которые используют сетевую карту в режиме, когда все пакеты, получаемые по физическим каналам, сетевой адаптер отправляет приложению для обработки. Работа снифферов осуществляется в сетях на законных основаниях и используются для диагностики неисправностей и анализа трафика. Но некоторые сетевые приложения передают данные в текстовом формате (например, FTP, SMTP, POP3 и т.д.), а это приводит к тому, что с помощью сниффера можно получить полезную, а в некоторых случаях и конфиденциальную информацию (например, имена пользователей и пароли).

Доступность таким образом имен и паролей может создать большую опасность, т.к. пользователи часто имеют одни и те же идентификационные имя и пароль для работы с разными приложениями и системами. В большинстве случаев у пользователя вообще есть только один пароль для доступа ко всем ресурсам и приложениям. Когда приложение работает в режиме клиент/сервер и аутентификационные данные передаются по сети в читаемом текстовом формате, то эта информация также может быть использована для доступа к другим корпоративным или внешним ресурсам. Если такой пароль становится известен (случайно или после целенаправленных действий), то постороннее лицо может получить доступ к важной информации. В самом

худшем случае может оказаться доступен пользовательский ресурс на системном уровне и получен доступ в сеть и к ее ресурсам.

Частично решить угрозу sniffфинга пакетов можно применением следующих действий:

- усложнение процесса аутентификация: например, использование однократных паролей (one-time passwords, OTP). Одним из аналогов является работа обычного банкомата, который производит идентификацию по пластиковой карточке и затем по вводимому ПИН-коду. Для аутентификации в системе OTP также требуется две составляющие – в качестве "карточки" (token) рассматривается аппаратное или программное средство, генерирующее (по случайному принципу) уникальный одномоментный однократный пароль. Получение этого пароля с помощью sniffфера окажется бесполезным, потому что использованный пароль больше не применяется. Однако, это позволяет устранить только перехват паролей.
- применение средств коммутации в сети: несанкционированный доступ может быть получить только к трафику, поступающему на один порт, что ограничивает угрозу sniffфинга, но не исключает его для этого порта.
- анти-sniфферы (например, AntiSniff): включение в общую систему защиты сети аппаратных или программных средств, распознающих sniffферы, работающие в этой сети. Их работа основана на измерении времени реагирования серверов и определении случаев обработки "дополнительного" трафика.
- криптография – возможность перехвата не предотвращается, но перехватывается не сообщение, а зашифрованный текст (то есть закодированная последовательность битов). К криптографическим протоколам сетевого управления относятся протоколы IPSec, SSH (Secure Shell) и SSL (Secure Socket Layer).

Одной из разновидностью атак являются парольные. Они могут проводиться с помощью целого ряда методов, таких как простой перебор (brute force attack), троянский конь и sniffфинг пакетов. Хотя идентификационное имя и пароль часто можно получить при помощи sniffфинга пакетов, часто

пытаются их подобрать, используя многочисленные попытки доступа. Такой подход и носит название простого перебора. Часто для такой атаки используется специальная программа, которая пытается получить доступ к ресурсу общего пользования (например, к серверу). Если в результате открывается доступ к ресурсам, то используются права того пользователя, пароль которого был подобран, при этом может не помочь даже последующее изменение пароля и идентификационного имени пострадавшим пользователем, т.к. "профессиональный" злоумышленник сможет активизировать свою работу в сети по уже имеющейся в его распоряжении информации.

Избежать парольных атак можно, если не применять пароли в текстовой форме. Одноразовые пароли и/или криптографическая аутентификация в большинстве случаев ликвидируют угрозу подобных атак.

При использовании обычных паролей, следует соблюдать определенные правила, затрудняющие их подбор:

- минимальная длина пароля должна быть не менее восьми символов;
- пароль должен включать символы верхнего регистра, цифры и специальные символы (#, %, \$ и т.д.);
- желательно не использовать свое имя и имена знакомых, а также связанные с биографией даты, числа, указывающие место жительства, и т.п.

Ряд полезных сведений можно получить на сервере группы экстренного реагирования на компьютерные проблемы CERT (Computer Emergency Response Team), в частности по борьбе с атаками DoS (http://www.cert.org/tech_tips/denial_of_service.html).

Кроме непосредственных атак возможно проведение *сетевой разведки* – сбора информации о сети с помощью общедоступных данных и приложений. При подготовке атаки против какой-либо сети злоумышленнику желательно 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 серверы реально работают. Получив список серверов, хакер использует средства сканирования портов,

чтобы составить полный список услуг, поддерживаемых этими серверами. Затем анализируются характеристики приложений, работающих на серверах. В результате добывается информация, которую можно использовать для взлома сети.

Полностью избавиться от сетевой разведки невозможно. Если отключить эхо ICMP, то будут потеряны данные, необходимые для диагностики сетевых сбоев. Системы обнаружения атак (IDS) на уровне сети и серверов обычно хорошо справляются с задачей уведомления администратора о ведущейся сетевой разведке, что позволяет лучше подготовиться к предстоящей атаке и оповестить того провайдера, в сети которого установлена система, проявляющая чрезмерное любопытство.

Часто встречается так называемое "злоупотребление доверием", не являющееся "атакой" или "штурмом". Просто происходит злонамеренное использование отношений доверия, существующих в сети, например, может возникнуть следующая ситуация в одной из частей корпоративной сети. Пусть в сегменте сети находятся серверы DNS, SMTP или HTTP. Т.к. они принадлежат к одному сегменту, то проникновение на один из них позволит получить доступ ко всем остальным, т.к. серверы "доверяют" другим системам своей сети. Риск злоупотребления доверием можно снизить за счет более жесткого контроля уровней доверия в пределах сети.

Для проникновения в корпоративную сеть могут использоваться разные вирусы (см. следующий раздел) и приложения типа "троянский конь". "Троянский конь" – это не программная вставка, а настоящая программа, которая выглядит как полезное приложение, а на деле выполняет вредную роль. Выполнившись на рабочей станции пользователя, приложение получает полную информацию о работе пользователя и формирует сообщения, отправляемые по электронной почте абонентам, заинтересованным в их получении.

Борьба с вирусами и "троянскими конями" ведется с помощью эффективного антивирусного программного обеспечения, работающего на пользовательском уровне и на уровне сети.

Как уже отмечалось, в функции межсетевых экранов закладывается организация защиты от удаленных атак. Однако, учитывая большую стоимость

данных продуктов, а также появление все новых и новых видов атак, для организации надежной защиты в последнее время стали применять и специализированные средства, получившие названия систем обнаружения атак. Основной задачей такого рода систем является постоянный мониторинг сетевой активности и выявление любых подозрительных событий. Должна быть предусмотрена и адекватная реакция на все такие события. Примером такого рода продуктов может служить система SAFESuite, состоящая из системы обнаружения атак RealSecure, систем анализа защищенности Internet Scanner, System Scanner и Database Scanner, а также системы поддержки принятия решений в области безопасности SAFESuite Decisions от фирмы Internet Security Systems (ISS), Inc. Фирма ISS выпустила обновления своих продуктов еще в декабре 1999 года, за 2 месяца до нашествивших атак на Amazon.com, Buy.com и других, и если бы вышеперечисленные порталы воспользовались бы продуктами этой фирмы, ничего подобного не произошло.

Доли основных поставщиков на мировом рынке систем обнаружения атак (IDS) в 1999 г. представлены на рис. 12.

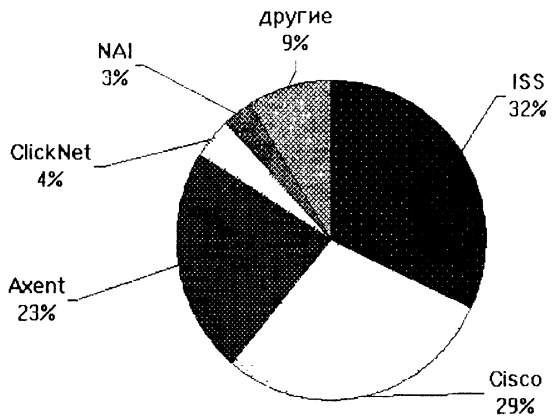


Рис. 12. Доли поставщиков IDS

В табл. 1 показано соответствие между имеющимися средствами безопасности и Интернет-сервисами, которые часто используются в различных организациях. Крестики в ячейках показывают, какие средства безопасности часто используются для организации безопасной работы данного сервиса. Некоторые из средств, такие как улаживание последствий инцидентов с безопасностью, обеспечивают безопасность для всех сервисов, в таких случаях знак стоит напротив тех сервисов, для которых данное средство необходимо.

Таблица 1. Использование средств безопасности для защиты сервисов

	Идентификация и аутентификация	Управление доступом	Брандмауэр	Средства контроля импортируемых программ	Шифрование	Архитектура	Устранение последствий инцидентов	Организационные меры
Удаленный доступ	X	X	X		X			X
Электронная почта	X			X	X			X
Публикация информации		X	X			X		X
Исследования		X	X	X		X		X
Электронная коммерция	X	X	X	X	X	X	X	X
Постоянная доступность						X		X
Легкость использования						X		X

6. Что такое компьютерный вирус? Распространение и проявление вирусов.

Считается, что термин "компьютерный вирус" впервые употребил сотрудник Лехайского университета (США) Ф. Козн на конференции по безопасности информации в 1984 г. Однако, еще в работах и фон Неймана исследовались различные виды конечных автоматов, в том числе и самовоспроиз-

водящихся. В любом случае, в настоящий момент эти вопросы представляют чисто исторический интерес и имеют мало отношения к реальности.

Компьютерный вирус – это специально написанная небольшая по размерам программа, которая может "приписывать" себя к другим программам (т.е. "заражать" их), а также выполнять различные нежелательные действия на компьютере. Даже это довольно простое утверждение способно развеять многочисленные легенды о необыкновенных возможностях компьютерных вирусов. Компьютерный вирус может перевернуть изображение на мониторе, но не может перевернуть сам монитор. К разговорам о вирусах "25 кадра", убивающих операторов, также следует относиться адекватно. Компьютерные вирусы это программы, обладающие способностью к самовоспроизведению. Указанное свойство присуще всем типам компьютерных вирусов, но не только им. Кроме того, способность к самовоспроизведению надо понимать весьма широко. Различные экземпляры одного вируса не только не обязаны полностью совпадать, но могут даже не иметь ни одного общего байта. Сами механизмы воспроизведения тоже могут быть весьма разнообразны.

Программа, внутри которой находится вирус, называется зараженной. Когда такая программа начинает работу, то сначала управление получает вирус. Вирус находит и "заражает" другие программы, а также выполняет какие-нибудь вредные действия (например, портит файлы или таблицу размещения файлов (FAT – File Allocation Table) на диске, "засоряет" оперативную память и т.д.). Для маскировки вируса действия по заражению других программ и нанесению вреда могут выполняться не всегда, а скажем, при выполнении определенных условий. После того как вирус выполнит нужные ему действия, он передает управление той программе, в которой он находится, и она работает как обычно. Тем самым внешне работа зараженной программы выглядит так же, как и незараженной.

Многие разновидности вирусов устроены так, что при запуске зараженной программы вирус остается в памяти компьютера и время от времени заражает программы и выполняет нежелательные действия на компьютере.

Существует совершенно формальная система, позволяющая классифицировать компьютерные вирусы и называть их таким образом, чтобы избежать ситуации, когда один и тот же вирус имеет неузнаваемо разные имена в

классификации разных разработчиков антивирусных программ. Несмотря на это, все еще нельзя сказать о полной унификации имен и характеристик вирусов. В значительной степени это определяется тем, что к тому моменту, когда были сформулированы некоторые "правила игры", уже существовали антивирусные средства, работающие в собственной системе обозначений. Всеобщая унификация потребовала бы приложить значительные усилия и модифицировать программы и документацию. В ряде случаев это было сделано. Мы станем исходить из того, что обычному пользователю нет необходимости вникать во все тонкости функционирования вируса: объекты атаки, способы заражения, особенности проявления и пр. Но желательно знать, какими бывают вирусы, понимать общую схему их работы.

6.1. Группы и виды вирусов.

Среди всего разнообразия вирусов можно выделить следующие основные группы, которые представлены в табл. 2.

Таблица 2. Основные группы вирусов

Группа вирусов	Что делает
Загрузочные (BOOT – Бутовые)	Заражают Boot-sector винчестера или дискеты и загружаются каждый раз при начальной загрузке операционной системы.
Файловые	Заражают исполняемые файлы. Могут вообще не модифицировать файл (вирусы-спутники и вирусы семейства Dir). Кроме того, к файловым относятся так называемые masco-вирусы.
Загрузочно-файловые	Обладают способностью заражать как код загрузочных секторов, так и код файлов.

Как правило, пользователи не замечают появления вирусов на компьютере и начала их активизации, а сталкиваются уже с внешними проявлениями компьютерных вирусов. Рассмотрим некоторые качественно важные виды и свойства компьютерных вирусов, сгруппированные в табл. 3.

Таблица 3. Свойства компьютерных вирусов

Резидент- ный вирус	Вирус который загружается в память компьютера и постоянно находится там до выключения компьютера.
Самомоди- фицирую- щийся (по- лиморф- ный) вирус	Изменяет свое тело таким образом, чтобы антивирусная программа не смогла его идентифицировать. Код зашифрован и представляет собой бессмысленный набор команд. Расшифровка производится самим вирусом уже непосредственно во время выполнения. При этом возможны самые различные варианты: вирус может расшифровать себя всего сразу, а может выполнять такую расшифровку "по ходу дела", может вновь шифровать уже отработавшие участки (причем иногда не тем способом, каким они были зашифрованы раньше) – в общем, имеется очень много различных вариантов. Все это делается только ради того, чтобы затруднить анализ кода вируса.
Stealth (невиди- мый) вирус	Так называют маскирующиеся вирусы. Видов маскировки великое множество, но все они основаны на перехвате вирусами прерываний BIOS и операционной системы. Перехватив прерывания, вирусы контролируют доступ к зараженным объектам.
macro-ви- русы	Файловые вирусы, заражающие файлы некоторых систем документооборота. Есть для MS Word (около 90%), Excel for Windows и AmiPro. Все указанные системы имеют встроенные макро-языки (Word Basic, Visual Basic). Эти языки обладают достаточными возможностями, чтобы производить практически все операции, необходимые вирусу. Имеются шифрованные и полиморфные macro-вирусы.

Все действия вируса могут выполняться очень быстро и без выдачи каких-либо сообщений, по этому пользователю очень трудно, практически невозможно, определить, что в компьютере происходит что-то необычное.

Пока на компьютере заражено относительно мало программ, наличие вируса может быть практически незаметным. Однако по прошествии некоторого времени на компьютере начинает твориться что-то странное, например:

- некоторые программы перестают работать или начинают работать неправильно;
- на экран выводятся посторонние сообщения, символы и т.д.;
- работа на компьютере существенно замедляется;
- некоторые файлы оказываются испорченными и т.д.

Некоторые вирусы ведут себя очень коварно. Они вначале незаметно заражают большое число программ и дисков, а затем наносят очень серьезные повреждения, например, форматируют весь жесткий диск на компьютере, естественно после этого восстановить данные бывает просто невозможно. А бывают вирусы, которые ведут себя очень скрытно, и портят понемногу данные на жестком диске или сдвигают таблицу размещения файлов (FAT). К последним относится вирус OneHalf, имеющий множество модификаций.

Таким образом, если не принимать мер по защите от вируса, то последствия заражения могут быть очень серьезными. Например, в начале 1989г. вирусом, написанным американским студентом Моррисом, были заражены и выведены из строя тысячи компьютеров, в том числе принадлежащих министерству обороны США. Автор вируса был приговорен судом к трем месяцам тюрьмы и штрафу в 270 тыс. дол. Наказание могло быть и более строгим, но суд учел, что вирус не портил данные, а только размножался.

Для того, чтобы программа-вирус была незаметной, она должна иметь небольшие размеры. По этому вирусы пишут обычно на низкоуровневых языках Ассемблер или низкоуровневыми командами языка Си.

6.2. Распространение вирусов.

Компьютерный вирус может испортить, т.е. изменить ненадлежащим образом, любой файл на имеющихся в компьютере дисках. Но некоторые виды файлов вирус может "заразить". Это означает, что вирус может "внедриться" в эти файлы, т.е. изменить их так, что они будут содержать вирус, который при некоторых обстоятельствах может начать свою работу.

Следует заметить, что тексты программ и документов, информационные файлы баз данных, таблицы табличных процессоров и другие аналогичные файлы не могут быть заражены обычным вирусом, он может их только ис-

портить. Заражение подобных файлов делается только Макро-вирусами. Эти вирусы могут заразить даже ваши документы.

Обычным вирусом могут быть заражены следующие виды файлов:

1. Исполняемые файлы, т.е. файлы с расширениями имен ".com" и ".exe", а также оверлейные файлы, загружаемые при выполнении других программ. Вирусы, заражающие файлы, называются *файловыми*. Вирус в зараженных исполняемых файлах начинает свою работу при запуске той программы, в которой он находится. Наиболее опасны те вирусы, которые после своего запуска остаются в памяти резидентно – они могут заражать файлы и вредить до следующей перезагрузки компьютера. А если они заразят любую программу, запускаемую из файла AUTOEXEC.BAT или CONFIG.SYS, то и при перезагрузке с жесткого диска вирус снова начнет свою работу.
2. Загрузчик операционной системы и главная загрузочная запись жесткого диска. Вирусы, поражающие эти области, называются *загрузочными* или *BOOT-вирусами*. Такой вирус начинает свою работу при начальной загрузке компьютера и становится резидентным, т.е. постоянно находится в памяти компьютера. Механизм распространения – заражение загрузочных записей вставляемых в компьютер дискет. Часто такие вирусы состоят из двух частей, поскольку загрузочная запись имеет небольшие размеры и в них трудно разместить целиком программу вируса. Часть вируса располагается в другом участке диска, например в конце корневого каталога диска или в кластере в области данных диска (обычно такой кластер объявляется дефектным, чтобы исключить затирание вируса при записи данных на диск).
3. Драйверы устройств, т.е. файлы, указываемые в предложении DEVICE файла CONFIG.SYS. Вирус, находящийся в них начинает свою работу при каждом обращении к соответствующему устройству. Вирусы, заражающие драйверы устройств, очень мало распространены, поскольку драйверы редко переписывают с одного компьютера на другой. То же относится и к системным файлам DOS (MSDOS.SYS и IO.SYS) – их заражение также теоретически возможно, но для распространения вируса малоэффективно.

Как правило, каждая конкретная разновидность вируса может заражать только один или два типа файлов. Чаще всего встречаются вирусы, заражающие исполняемые файлы. На втором месте по распространенности загрузочные вирусы. Некоторые вирусы заражают и файлы и загрузочные области дисков. Вирусы, заражающие драйверы устройств, встречаются крайне редко, обычно такие вирусы умеют заражать и исполняемые файлы.

7. Меры защиты от компьютерных вирусов.

Для защиты от вирусов можно использовать:

- общие средства защиты информации, которые полезны также как страховка от физической порчи дисков, неправильно работающих программ или ошибочных действий пользователей;
- профилактические меры, позволяющие уменьшить вероятность заражения вирусом;
- специализированные программы для защиты от вирусов.

Общие средства защиты информации полезны не только для защиты от вирусов. Имеются две основные разновидности этих средств:

копирование информации – создание копий файлов и системных областей дисков;

разграничение доступа предотвращает несанкционированное использование информации, в частности, защиту от изменений программ и данных вирусами, неправильно работающими программами и ошибочными действиями пользователей.

Несмотря на то, что общие средства защиты информации очень важны для защиты от вирусов, все же их одних недостаточно. Необходимо применять специализированные программы для защиты от вирусов. Эти программы можно разделить на несколько видов:

1. Программы-детекторы (scanner) позволяют обнаруживать файлы, зараженные одним из нескольких известных вирусов.
2. Программы-доктора или фаги "лечат" зараженные программы или диски, "выкусывая" из зараженных программ тело вируса, т.е. восстанавливая программу в том состоянии, в котором она находилась до заражения вирусом.

3. Программы-ревизоры сначала запоминают сведения о состоянии программ и системных областей дисков, а затем сравнивают их состояние с исходным. При выявлении несоответствий, об этом сообщается пользователю.
4. Доктора-ревизоры – это гибриды ревизоров и докторов, т.е. программы, которые не только обнаруживают изменения в файлах и системных областях дисков, но и могут автоматически вернуть их в исходное состояние.
5. Программы-фильтры или сторожа располагаются резидентно в оперативной памяти компьютера и перехватывают те обращения к операционной системе, которые используются вирусами для размножения и нанесения вреда, и сообщают о них пользователю. Пользователь может разрешить или запретить выполнение соответствующей операции.
6. Программы-вакцины или иммунизаторы модифицируют программы и диски таким образом, что это не отражается на работе программ, но вирус, от которого производится вакцинация, считает эти программы и диски уже зараженными. Эти программы считаются неэффективными.
7. Аппаратные средства защиты – специальные дополнительные устройства, обеспечивающие достаточно надежную (в некотором смысле – абсолютную) защиту. В отличие от всех рассмотренных выше антивирусных средств, например, плата Sheriff способна предотвратить нападение вируса. К сожалению, известны случаи, когда пользователи, установившие на компьютере плату Sheriff, были настолько уверены в своей полной неуязвимости, что совершенно теряли всякую осторожность, не обращая внимания на области жесткого диска, не защищенные Sheriff (а такие области есть практически всегда).

7.1. Стратегия защиты от вирусов.

Ни один тип антивирусных программ по отдельности не дает, к сожалению, полной защиты от вирусов. По этому наилучшей стратегией защиты от вирусов является многоуровневая, "эшелонная" оборона. Необходимо помнить, что антивирусные средства должны применяться комплексно и только такая комплексная защита с использованием надежного ревизора (ADInf), фаров Doctor Web и Aidstest, а при необходимости и платы Sheriff способна

обеспечить максимальную безопасность. Опишем структуру подобной обороны.

Средствам разведки в "обороне" от вирусов соответствуют программы – детекторы, позволяющие проверять вновь полученное программное обеспечение на наличие вирусов.

На переднем крае обороны находятся программы–фильтры (резидентные программы для защиты от вируса). Эти программы могут первыми сообщить о вирусной атаке и предотвратить заражение программ и диска.

Второй эшелон обороны составляют программы–ревизоры, программы–доктора и доктора–ревизоры. Ревизоры обнаруживают нападение даже тогда, когда вирус сумел "просочиться" через передний край обороны. Программы–доктора применяются для восстановления зараженных программ, если ее копий нет в архиве. Но они не всегда лечат правильно. Доктора–ревизоры обнаруживают нападение вируса и лечат зараженные файлы, причем контролируют правильность лечения.

Самый глубокий эшелон обороны – это средства разграничения доступа. Они не позволяют вирусам и неверно работающим программам, даже если они проникли в компьютер, испортить важные данные.

И, наконец, в "стратегическом резерве" находятся архивные копии информации и "эталонные" дискеты с программными продуктами. Они позволяют восстановить информацию при ее повреждении на жестком диске.

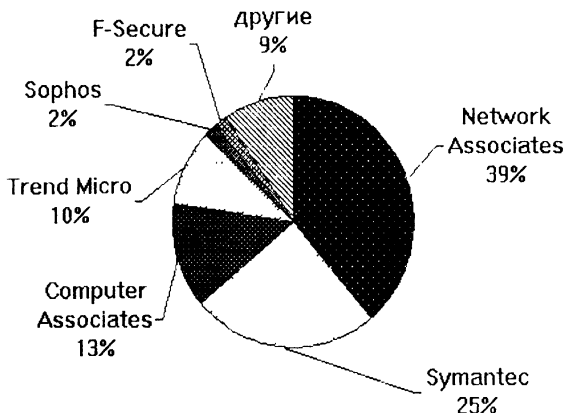


Рис. 13. Соотношение поставщиков антивирусов

На рис. 13 представлена информация о соотношении доходов поставщиков антивирусов на мировом рынке в 1999 г.

Результаты реализации антивирусных средств на мировом рынке с 1999г. и прогнозируемая динамика доходов от их продажи до 2004г. изображены на рис. 14.

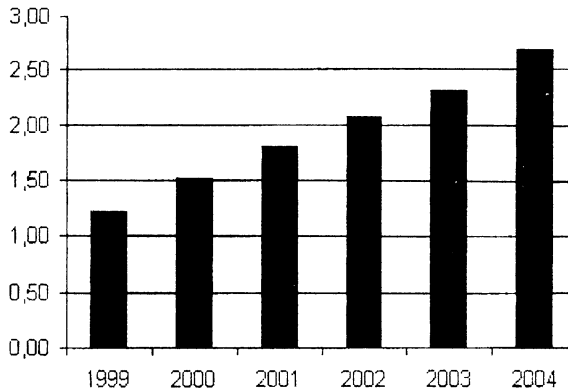


Рис. 14. Доходы (в млрд. долларов) на мировом рынке антивирусов

8. Понятия и статьи уголовного кодекса, связанные с информационной безопасностью.

Все описанные выше средства обеспечения компьютерной и информационной безопасности могут быть успешно применены только в случае поддержки их законодательной базой. Конечно, в настоящий момент, такой базис еще не достаточно совершенен, но все же он есть. В заключение предлагается познакомиться и проанализировать несколько понятий и статей из российского законодательства и уголовного кодекса, посвященные последствиям получения несанкционированного доступа к компьютерной информации.

Блокирование компьютерной информации – искусственное затруднение доступа пользователей к информации, не связанное с ее уничтожением.

Копирование компьютерной информации – повторение и устойчивое запечатление информации на машинном или ином носителе.

Модификация компьютерной информации – внесение любых изменений, кроме связанных с адаптацией программы для ЭВМ или баз данных.

Несанкционированное уничтожение, блокирование, модификация, копирование информации – любые не разрешенные законом, собственником или компетентным пользователем указанные действия с информацией.

Обман (отрицание подлинности, навязывание ложной информации) – умышленное искажение или сокрытие истины с целью ввести в заблуждение лицо, в ведении которого находится имущество и таким образом добиться от него добровольной передачи имущества, а также сообщение с этой целью заведомо ложных сведений.

Повреждение – изменение свойств имущества, при котором существенно ухудшается его состояние, утрачивается значительная часть его полезных свойств и оно становится полностью или частично непригодным для целевого использования.

Уничтожение – внешнее воздействие на имущество, в результате которого оно прекращает свое физическое существование либо приводится в полную непригодность для использования по целевому назначению. Уничтоженное имущество не может быть восстановлено путем ремонта или реставрации и полностью выводится из хозяйственного оборота.

Уничтожение компьютерной информации – стирание ее в памяти ЭВМ.

Исцещение – совершенные с корыстной целью противоправные безвозмездное изъятие и (или) обращение чужого имущества в пользу виновного или других лиц, причинившее ущерб собственнику или владельцу имущества.

Статья 272. Неправомерный доступ к компьютерной информации.

Неправомерный доступ к охраняемой законом компьютерной информации, то есть информации на машинном носителе, в электроно-вычислительной машине (ЭВМ), системе ЭВМ или их сети, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети, – наказывается штрафом в размере от двухсот до пятисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от двух до пяти месяцев, либо исправительными работами на срок от шести месяцев до одного года, либо лишением свободы на срок до двух лет.

То же деяние, совершенное группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, а равно имеющим доступ к ЭВМ, системе ЭВМ или их сети, – наказывается штрафом в размере от пятисот до восьмисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от пяти до восьми месяцев, либо исправительными работами на срок от одного года до двух лет, либо арестом на срок от трех до шести месяцев, либо лишением свободы на срок до пяти лет.

Статья 273. Создание, использование и распространение вредоносных программ для ЭВМ.

Создание программ для ЭВМ или внесение изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети, а равно использование либо распространение таких программ или машинных носителей с такими программами – наказывается лишением свободы на срок до трех лет со штрафом в размере от двухсот до пятисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от двух до пяти месяцев.

Те же деяния, повлекшие по неосторожности тяжкие последствия, – наказываются лишением свободы на срок от трех до семи лет.

Статья 274. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети.

Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети лицом, имеющим доступ к ЭВМ, системе ЭВМ или их сети, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ, если это деяние причинило существенный вред, – наказывается лишением права занимать определенные должности или заниматься определенной деятельностью, на срок до пяти лет, либо обязательными работами на срок от ста восьмидесяти до двухсот сорока часов, либо ограничением свободы на срок до двух лет. То же деяние, повлекшее по неосторожности тяжкие последствия, – наказывается лишением свободы на срок до четырех лет.

Средства информационной безопасности.

1. Системы анализа защищенности:
Database Scanner, Internet Scanner, Online Scanner, Desktop Scanner и System Scanner (фирма ISS); Cisco Secure Scanner (фирма Cisco).
2. Средства антивирусной защиты:
Dr.Web (Лаборатория Данилова и ДиалогНаука)
Антивирус Касперского (Лаборатория Касперского).
3. Средства аутентификации/авторизации:
Cisco Secure Access Control Server (фирма Cisco).
4. Межсетевые экраны:
Firewall-1, Firewall-1 Secure Server, Reporting Module, Open Security Extension, LDAP Account Management, High Availability Module, Connect Control Module, Visual Policy Editor, Provider-1, MultiGate-1 и OPSEC (фирма Check Point); Cisco Secure PIX Firewall и IOS Firewall Feature Set (фирма Cisco).
5. Средства построения виртуальных частных сетей (VPN)
VPN-1 v4.1, VPN-1 SecureClient, VPN-1 SecureServer и VPN-1 SecuRemote (фирма Check Point).
6. Системы обнаружения атак (IDS):
RealSecure (фирма ISS), Cisco Secure Intrusion Detection System (фирма Cisco).
7. Средства мониторинга и фильтрации содержимого электронной почты и WEB-ресурсов:
MAILsweeper для SMTP, WEBSweeper, PORNsweeper, SECRETsweeper, MIMESweeper для Domino, MAILsweeper для Exchange и e-Sweeper (фирма Baltimore).
8. Системы безопасности на основе цифровых сертификатов:
SSL-сертификаты (фирма Thawte); Public Key Infrastructure (фирма RSA Security; UniCERT (фирма Baltimore).
9. Системы управления безопасностью:
SAFEsuite Decisions (фирма ISS).

Приложение 2.

Перечень информационных ресурсов Интернет,
посвященных вопросам информационной безопасности.

Зарубежные узлы:

First (Forum of Incident Response and Security Teams)	http://www.first.org
CERT (Computer Emergency Response Team)	http://www.cert.org
CIAC (Computer Incident Advisory Capability)	http://www.ciac.org/cia
Фирма Cisco	http://www.cisco.ru
NASIRC (NASA Automated Systems Incident Response Capability)	http://nasirc.nasa.gov
NSA (National Security Agency)	http://www.nsa.gov:8080
FBI Computer crime information	http://www.fbi.gov
Bugtrad	http://www.securityfocus.com
LOpht Heavy Industries (AntiSniff)	http://www.l0pht.com/antisniff/
COAST (Computer Operations, Audit, and Security Technology)	http://www.cs.purdue.edu/coast

Отечественные узлы:

ИКСИ (Институт криптографии, связи и информатики)	http://www.fssr.ru
Dr.Web	http://www.drweb.ru
Лаборатория Касперского	http://www.kaspersky.ru
СЦЗИ (Специализированный Центр Защиты Информации при СПбГТУ)	http://www.ssl.stu.neva.ru
Spy Market Pro	http://www.spymarket.com
Zhurnal.ru	http://www.zhurnal.ru/hack-zone

Заключение

В связи с глобальным использованием компьютерных технологий и связанными с этим переменами в современном обществе существенно возрастает значение информационной культуры. Информатизация разных сторон российского общества, использование услуг глобальной сети Интернет во многих сферах производственной и предпринимательской деятельности (финан-

сы, торговля, включая электронный бизнес, и т.п.), внедрение компьютерных технологий в системы управления выдвигают на первый план проблемы информационной безопасности предприятий и организаций. При этом существует необходимость адаптации устоявшихся профессиональных и корпоративных норм, правил и стиля поведения к имеющейся в настоящее время информационной ситуации. Важной составляющей в корпоративной культуре любой организации является информационная безопасность, а также круг вопросов, связанных с ее обеспечением. Существенное влияние на нее может оказывать любой сотрудник даже самого незначительного подразделения, т.е. хочется подчеркнуть, что нельзя пренебрегать и человеческим фактором.

Для успешной защиты информационных интересов учреждения или фирмы требуется специалист по безопасности, который владеет комплексом проблем информационной безопасности, может определять стратегию и комплекс мероприятий по защите корпоративной сети организации от различных угроз, разбирается в технических средствах защиты информации, а также умеет работать с людьми. Как ни странно, но типичные угрозы информационной безопасности обычно исходят от "внутреннего врага", а компьютерная техника страдает от простой небрежности или невнимательности при ее эксплуатации. Даже компетентные и аккуратные пользователи могут причинить вред. Например, для улучшения результатов своей работы они могут получить из глобальной сети файл, содержащий вирус, или случайным образом сообщить свой пароль потенциальным компьютерным злоумышленникам, а это переводит личные трудности отдельного сотрудника уже в реальную угрозу информационной безопасности всей организации в целом.

Повышение информационной безопасности зависит, прежде всего, от всех сотрудников, их информационной культуры, социальной и профессиональной ответственности за соблюдение информационно-безопасного режима работы. Данное учебное пособие обеспечивает, по мнению авторов, введение в проблематику информационной безопасности, получение первоначальных сведений по возможным угрозам и мерам по защите от их воздействия, должно нацелить читателя на ответственное применение компьютерных технологий. Профессиональная подготовка по этому направлению, включающая детальное рассмотрение аппаратных и программных методов защиты информации и компьютерных сетей предусмотрена при прохождении специальных дисциплин.

Терминологическая справка

Архитектура клиент/сервер – структура служб Интернета или корпоративной сети. Клиент запрашивает у сервера WEB необходимые ресурсы и данные. Кроме того, приложения могут запускаться на сервере WEB, а результаты их выполнения будут передаваться клиенту.

Банкомат – специализированное устройство, предназначенное для обслуживания клиента в отсутствие банковского персонала; является составной частью банковской системы и предназначен, в основном, для выдачи наличных денег.

Интернет-провайдер (Internet Provider, от англ. provide – обеспечивать, предоставлять) – организация, предоставляющая пользователям определенные Интернет-услуги, например, WWW, E-Mail, FTP, Newsgroups, т.е. обеспечивает доступ к сети Интернет, и возможно, предоставляет другие Интернет-услуги.

Источник угрозы – это потенциальные антропогенные, техногенные или стихийные носители угрозы безопасности.

Компьютерный вирус – это специально написанная небольшая по размерам программа, которая может "приписывать" себя к другим программам (т.е. "заражать" их), а также выполнять различные нежелательные действия на компьютере.

Кракер (crackers) – лицо, непосредственно осуществляющее компьютерный взлом с целью получения несанкционированного доступа к закрытым для него информационным ресурсам и частям системы. Кракеры делятся на *вандалов* (осуществляют проникновение в систему с целью полного ее уничтожения), *"шутников"* (после проникновения в систему оставляют следы своего пребывания в виде различных эффектов с целью заявить о своих способностях и стать известными) и *взломищиков* (профессионалов по взлому систем с определенными целями, например, кражи или подмены информации для получения выгоды).

Персональный идентификационный номер ПИН – код (Personal Identification Number, PIN) – это последовательность цифр, используемая для идентификации клиента (владельца пластиковой карты).

Последствия или атака – это возможные последствия реализации угрозы (действия) при взаимодействии источника угрозы через имеющиеся факторы (уязвимости).

Угроза или действие (Threat) – это возможная опасность (потенциальная или реально существующая) совершения какого-либо деяния (действия или бездействия), направленного против объекта защиты (информационных ресурсов), наносящего ущерб собственнику, владельцу или пользователю, проявляющегося в опасности искажения и потери информации.

Уязвимость или фактор (Vulnerability) – это присущие объекту информатизации причины, приводящие к нарушению безопасности информации на конкретном объекте и обусловленные недостатками процесса функционирования объекта информатизации, свойствами архитектуры автоматизированной системы, протоколами обмена и интерфейсами, применяемыми программным обеспечением и аппаратной платформой, условиями эксплуатации.

Хакер (hacker) – профессиональный программист, который целенаправленно изучает детали функционирования компьютерных систем для расширения их возможностей, а также обнаружения слабых мест в их защите и поиска уязвимостей в вычислительных системах путем осуществлением атак. Его деятельность направлена на извлечение собственной выгоды, повышение своего уровня и информирование разработчиков программного обеспечения об обнаруженных в нем недостатках.

POS (point-of-sale) – системы, обеспечивающие расчеты продавца и покупателя в точке продажи или оказания услуги, включая проверку и обслуживание дебетовых и кредитных карточек, использование системы электронных расчетов.

TCP/IP (Transmission Control Protocol/Internet Protocol) – сетевой протокол, позволяющий компьютерам осуществлять соединения по внутренним сетям или через Интернет. Каждый компьютер в Интернете использует TCP/IP.

Литература

1. Айков Д. и др. Компьютерные преступления. Руководство по борьбе с компьютерными преступлениями. – Мир, 1999.
2. Анин Б.Ю. Защита компьютерной информации. – СПб.: BHV, 2000.
3. Блэк У. Интернет: протоколы безопасности. Учебный курс. – СПб.: Питер.
4. Бэчманн В., Монти Г., Стерн М. Сети предприятий на основе Windows NT для профессионалов. – СПб.: Питер, 1999.
5. Герасимов И.В., Калмычков В.А., Ларистов А.И., Лозовой Л.Н. Информатика. Учебно-методический комплекс по теме “Сетевые компьютерные технологии”: Учеб. пособие. – СПб.: Изд-во СПбГЭТУ «ЛЭТИ», 2001.
6. Дорот В.Н., Повиков Ф.А. Толковый словарь современной компьютерной лексики. Новейшие термины. – СПб.: BHV, 1999.
7. Еремин, Косарев, Компьютерные системы и сети. – М.: Финансы и статистика, 1999.
8. Зима В.М. и др. Безопасность глобальных сетевых технологий. – СПб.: BHV, 2001.
9. Косарев В.П. Компьютерные системы и сети. – М.: Финансы и статистика, 1999.
10. Милославская Н.Г. и др. Интрасети: доступ в Internet, защита. Учебное пособие для ВУЗов. – ЮНИТИ, 1999.
11. Молдовян А.А., Молдовян Н.А., Советов Б.Я. Криптография. – СПб.: Издательство “Лань”, 2001.
12. Молдовян Н.А. Проблематика и методы криптографии. – СПб.: СПбГУ, 1998.
13. Найк Д. Стандарты и протоколы Интернета. – Ченнел Трейдинг Лимитед, 1999.
14. Олифер В. Г., Олифер И. А. Компьютерные сети: принципы, технологии, протоколы. – СПб.: Питер, 2001.
15. Соколов А.В. Методы информационной защиты объектов и компьютерных сетей. – Полигон, 2000.
16. Устинов Г.Н. Основы информационной безопасности систем и сетей передачи данных. – СИИТЕГ, 2000.
17. Хан Х. Желтые страницы Internet & Web 2001. Международные ресурсы. – СПб.: Питер, 2001.

ОГЛАВЛЕНИЕ

Введение.....	3
1. Понятие информационной безопасности.....	4
2. Угрозы информационной безопасности.....	9
3. Средства защиты информации в ЛВС.....	12
3.1. Технические средства защиты.....	13
3.2. Программные средства защиты.....	13
3.3. Криптографические средства защиты.....	15
3.4. Организационные средства защиты.....	17
3.5. Законодательные средства защиты.....	17
4. Права пользователя и защита корпоративной сети.....	18
4.1. Идентификация пользователя при удаленном обслуживании.....	18
4.2. Механизмы защиты информации в корпоративной сети.....	22
5. Безопасность корпоративной сети при выходе в Интернет.....	25
5.1. Мероприятия по обеспечению безопасности.....	26
5.2. Межсетевой экран.....	28
5.3. Виды удаленных атак.....	34
6. Что такое компьютерный вирус?	
Распространение и проявление вирусов.....	45
6.1. Группы и виды вирусов.....	47
6.2. Распространение вирусов.....	49
7. Меры защиты от компьютерных вирусов.....	51
7.1. Стратегия защиты от вирусов.....	52
8. Понятия и статьи уголовного кодекса, связанные с информационной безопасностью.....	54
Приложение 1. Средства информационной безопасности.....	57
Приложение 2. Перечень информационных ресурсов Интернет, посвященных вопросам информационной безопасности.....	58
Заключение.....	58
Терминологическая справка.....	60
Литература.....	62

Герасимов Игорь Владимирович
Калмычков Виталий Анатольевич
Кочетков Андрей Валерьевич

ИНФОРМАТИКА

Учебно-методический комплекс по теме
“Информационная безопасность”
Учебное пособие

Редактор Э. К. Долгатов

ЛР N 020617 от 24.06.98

Подписано в печать 10.12.01 . Формат 60×84 1/16 . Бумага офсетная

Печать офсетная. Усл.печ.л. 3,72. Уч.-изд.л. 4.

Тираж 100 экз. Заказ 166

Издательство СПбГЭТУ «ЛЭТИ»
197376, С.-Петербург, ул. Проф. Попова, 5

Созданием файла в формате pdf
занимался ewgeniy-new
(июль 2014)