ГЛАВА 11. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

11.1. Проблемы информационной безопасности

Проблема информационной безопасности возникла достаточно давно и имеет глубокие исторические корни. До сравнительно недавнего времени методы защиты информации были в исключительной компетенции спецслужб, обеспечивающих безопасность страны. Однако новые технологии измерения, передачи, обработки и хранения информации значительно расширили сферы деятельности людей, нуждающихся в защите информации, привели к развитию и распространению новых методов несанкционированного доступа к информации и, как следствие, к интенсивному развитию нового научного направления – «*информационная безопасность*». Все это связано, прежде всего, с появлением систем обработки данных на базе компьютеров, а также с бурным развитием систем передачи данных.

Можно выделить некоторые причины, которые и привели к необходимости как разработки новых методов защиты информации, так и к дальнейшему развитию традиционных.

Первые системы коллективного пользования ЭВМ, а затем объединение их в глобальные и локальные сети, технологии открытых систем уже на первом этапе выявили потребность в защите информации от случайных ошибок операторов, сбоев в аппаратуре, электропитании и т.п.

Стремительный рост емкости внешних запоминающих устройств и высокая эффективность их использования в системах автоматизированного управления привели к созданию банков (баз) данных колоссальной емкости и высокой стоимости, одновременно создавая проблемы их защиты, как от разнообразных случайностей, так и от несанкционированного доступа.

Современные информационные системы составляют техническую основу органов управления государственной власти, промышленных предприятий и научно-исследовательских организаций, учреждений кредитно-финансовой сферы, банков и т.п.

Сегодня, когда компьютер прочно вошел в наш быт, мы все чаще вынуждены доверять ему свои секреты (финансовые, промыш-

ленные, медицинские и др.), и в связи с этим вопросы защиты информации приобретают всеобъемлющий характер.

Кроме чисто технических задач разработки средств защиты информации имеются нормативно-технические, организационно-правовые, юридические и другие аспекты. Основные задачи, рассматриваемые специалистами по информационной безопасности (а также публикации на эту тему), связаны с обеспечением безопасности использования глобальных и локальных сетей, с проблемами глобальной вычислительной сети Интернет, «хакерами», «вирусами» и т.п.

Резюмируя сказанное, можно выделить технические, организационные и правовые меры обеспечения информационной безопасности и предотвращения компьютерных преступлений.

К техническим мерам относятся:

защита от несанкционированного доступа;

резервирование особо важных компонентов подсистем;

организация вычислительных сетей с перераспределением ресурсов при временном нарушении работоспособности какой-либо части сети;

создание устройств обнаружения и тушения пожаров;

создание устройств обнаружения утечек воды;

техническая защита от хищений, саботажа, диверсий, взрывов;

дублирование электропитания;

надежные запирающие устройства;

устройства сигнализации о различных опасностях.

К организационным мерам относятся:

надежная охрана;

подбор надежного персонала;

правильная организация работы персонала;

предусмотренный план восстановления работы информационного центра после сбоя;

организация обслуживания и контроля работы компьютерного центра лицами, не заинтересованными в сокрытии преступлений;

создание средств защиты информации от любых лиц, включая и руководящий персонал;

предусмотренные меры административной и уголовной ответственности за нарушение правил работы;

правильный выбор местонахождения информационного центра с дорогостоящим техническим и программным обеспечением.

К правовым мерам относятся:

разработка уголовных норм ответственности за компьютерные преступления;

защита авторских прав программистов;

усовершенствование уголовного и гражданского законодательства;

усовершенствование судопроизводства по компьютерным преступлениям;

общественный контроль за разработчиками компьютерных систем;

принятие ряда международных соглашений, касающихся информационной безопасности.

Это очень крупная научно-техническая проблема и, естественно, мы не можем осветить ее в полной мере и коснемся только основных понятий, определений и средств защиты, доступных пользователю, причем начнем с наиболее близкой проблемы рядового пользователя – с сохранения информации, не связанного с несанкционированным доступом.

11.2. Защита информации от непреднамеренных воздействий

Рассмотрим некоторые приемы и методы, связанные с защитой информации от случайных ошибок или некомпетентности пользователей, а также от сбоев аппаратуры, в частности из-за помех в электросети, т.е. причин возможной потери информации, не связанных с несанкционированным доступом и происками злоумышленников. Потеря файлов, а также крах системы вполне возможны и без внешних, корыстных помыслов. В связи с этим во всех операционных системах предусматриваются простейшие средства профилактики. Так, при удалении файлов, как правило, требуется дополнительное подтверждение, а удаленный файл, как правило, при необходимости может быть восстановлен, поскольку определенное время он хранится в специальном буфере («корзина для мусора»).

Для того чтобы обезопасить себя от неприятных последствий (связанных с вышеперечисленными инцидентами), приводящих к потере данных на сервере или рабочих станциях, которые могут представлять большую ценность, так как являются результатом больших трудовых затрат, необходимо выполнение определенных мероприятий. Существует три основных способа защиты от таких воздействий – резервное копирование данных, избыточное дублирование и установка специализированных устройств защиты от нарушений в системе электропитания.

Резервное копирование данных. Методы, используемые для резервного копирования, зависят от их объема, важности информации и динамики ее изменения. Если говорить о носителях, применимых для хранения резервных копий, то дискеты годятся лишь в частных случаях для небольших объемов информации и личных архивов пользователей. В большинстве случаев используются либо накопители на магнитной ленте (стримеры), либо магнитно-оптические устройства, либо оптические типа WORM или WARM. Независимо от типа устройства для резервного копирования необходимо систематически проводить копирование данных во избежание их потери. Выбор конкретного способа зависит от того, как часто изменяются данные, какую ценность они представляют и как много времени потребуется для этой процедуры. Существуют следующие способы резервного копирования.

Случайный. При таком подходе производится случайное копирование отдельных файлов. Метод является наименее надежным, так как если обнаружится, что копия не самая новая, приходится проделать весь объем работы от момента изготовления этой резервной копии. Еще хуже, если носитель, на котором находится резервная копия, окажется поврежденным. Однако это лучше, чем ничего.

Серьезный. Резервные копии производятся регулярно и для их изготовления используются два набора носителей.

Профессиональный. Этот метод используют вычислительные центры с дорогостоящим оборудованием и большими компьютерами. В нем используются три копии данных на трех наборах носителей (для надежности иногда используются по два экземпляра для каждого из наборов). При работе поочередно используется каждый

из наборов. Этот метод иногда называют схемой «сын – отец – дед».

Избыточность данных. Резервирование также подразумевает избыточность данных. С точки зрения подлинности лучше иметь два средних размера файловых сервера в локальной сети, чем один большой. Тогда в случае выхода из строя одного из них можно временно продолжать работать с другим. Конечно же, при этом на втором сервере должны находиться резервные копии рабочих файлов.

Несмотря на то, что системы хранения данных, основанные на магнитных дисках, производятся уже 40 лет, массовое производство отказоустойчивых систем началось совсем недавно. Дисковые массивы с избыточностью данных, которые принято называть RAID (redundant arrays of inexpensive disks – избыточный массив недорогих дисков) были представлены исследователями (Петтерсон, Гибсон и Катц) из Калифорнийского университета в Беркли в 1987 г. Но широкое распространение RAID-системы получили только тогда, когда диски, которые подходят для использования в избыточных массивах, стали доступны и достаточно производительны. Со времени представления официального доклада о RAID в 1988 г. исследования в сфере избыточных дисковых массивов начали бурно развиваться, в попытке обеспечить широкий спектр решений на основе компромисса «цена – производительность – надежность».

С аббревиатурой RAID в свое время случился казус. Дело в том, что недорогими дисками во время написания статьи назывались все диски, которые использовались в персональных компьютерах, в противовес дорогим дискам для мейнфреймов. Но для использования в массивах RAID пришлось использовать достаточно дорогостоящую аппаратуру по сравнению с другой комплектацией персональных компьютеров, поэтому RAID начали расшифровывать как redundant array of independent disks – избыточный массив независимых дисков.

Производители файловых серверов, учитывая необходимость избыточности данных, предлагают модели с дисковыми массивами – системами НЖМД, в которых информация зеркально дублирована на различных дисководах. Естественно, что избыточность данных ни в коей мере не заменяет необходимость резервного копирования.

Защита от помех в электросети. Сбои электропитания всегда происходят неожиданно. В момент сбоя электросети практически любая программа может в какой-то степени испортить файл, с которым она работала. Для защиты от таких ситуаций необходимо использовать источники бесперебойного питания (UPS – Uninterruptable Power System) файл-серверов. Нет необходимости подключать к UPS рабочие станции, поскольку производители UPS нормируют их по максимальной мощности подключенных к ним приборов, так что не следует превышать эту величину.

После пропадания напряжения в электросети батареи UPS обеспечивают работоспособность сервера в последующие десять минут – время, достаточное для того, чтобы завершить работу и успеть сохранить рабочие файлы. Кроме того, UPS защищает файл-сервер от скачков напряжения в электросети.

Существуют и более дешевые системы дежурного питания (SPS – Standby Power System) вместе с фильтром напряжения сети, которые защищают оборудование от кратковременных исчезновений электроэнергии в электросети, выбросов и помех.

В современных критически важных серверах принято за правило устанавливать особые Redundant-блоки питания, которые предоставляют системному администратору возможность подключать сервер одновременно к двум источникам питания (например, к двум электрическим розеткам, подключенным к двум независимым электрическим группам, или одновременно к электрической розетке и к UPS). При падении напряжения на одном из подключений сервер продолжает работать на другом. Это намного повышает надежность питания сервера и позволяет производить плановую замену UPS без остановки сервера.

11.3. О некоторых понятиях компьютерной безопасности

Термины «информационная безопасность» (information security) и «безопасность сети» (network security) в широком смысле относятся к секретности, т.е. гарантии того, что информация и службы, имеющиеся в сети, не будут доступны для несанкционированного использования. Безопасность подразумевает механизм защиты, гарантирующий невозможность несанкционированного доступа к вычислительным ресурсам, шпионажа или перехвата сообщений, а

также работу служб. Конечно, нельзя гарантировать абсолютную безопасность сети, так же как нельзя гарантировать полную защищенность материальных ценностей.

Обеспечение информационной безопасности требует охраны как физических, так и виртуальных ресурсов. К физическим устройствам можно отнести такие пассивные устройства для хранения информации, как жесткие диски и компакт-диски, и такие активные устройства, как компьютеры пользователей. В сетевом окружении понятие физической безопасности относится к кабелям, мостам, маршрутизаторам и т.д. Хотя о физической безопасности упоминается очень редко, она часто играет важную роль при планировании полной безопасности, а меры по ее обеспечению достаточно традиционны и хорошо известны.

Обеспечение безопасности такого виртуального ресурса, как информация, обычно связывают с тремя основными понятиями компьютерной безопасности.

1. Угроза безопасности компьютерной системы – потенциально возможное происшествие, которое может оказать нежелательное воздействие на саму систему, а также на информацию, хранящуюся в ней.

Обычно выделяют три вида угроз.

Угроза раскрытия заключается в том, что информация становится известной нежелательным лицам. Иногда вместо слова «раскрытие» используют термины «кража» или «утечка».

Угроза целостности включает себя любое умышленное изменение (модификацию или даже удаление) данных, хранящихся в вычислительной системе или передаваемых из одной системы в другую. Обычно считается, что угрозе раскрытия подвержены в большей степени государственные структуры, а угрозе целостности – деловые или коммерческие.

Угроза отказов обслуживания возможна всякий раз, когда в результате определенных действий блокируется доступ к некоторому ресурсу вычислительной системы. Блокирование может быть постоянным (чтобы запрашиваемый ресурс никогда не был получен) или может вызвать только задержку, достаточно долгую для того, чтобы он стал бесполезным. В таких случаях говорится, что ресурс исчерпан. В локальных вычислительных системах наиболее частыми являются угрозы раскрытия и целостности информации, а в глобальных на первое место выходит угроза отказа от обслуживания.

2. Уязвимость компьютерной системы – некоторые ее неудачные характеристики, которые дают возможность возникновения угрозы. Именно из-за уязвимости в системе происходят нежелательные явления.

3. Атака на компьютерную систему – третье основополагающее понятие компьютерной безопасности. Это действие, предпринимаемое злоумышленником, которое заключается в поиске той или иной уязвимости. Таким образом, атака – реализация угрозы. К сетевым системам наряду с обычными (локальными) системами, осуществляемыми в пределах одной компьютерной системы, применим специфический вид атак, обусловленный распределенностью ресурсов и информации в пространстве – так называемые «сетевые (или удаленные) атаки». Они характеризуются, во-первых, тем, что злоумышленник находится за тысячи километров от атакуемого объекта, и, во-вторых, тем, что нападению может подвергаться не конкретный компьютер, а информация, передающаяся по сетевым соединениям. С развитием локальных и глобальных сетей именно удаленные атаки считаются лидирующими по количеству попыток и по успешности их применения, поэтому обеспечение безопасности с точки зрения противостояния сетевым атакам приобретает первостепенное значение.

Под *удаленной атакой* обычно понимается информационное воздействие на распределенную вычислительную систему, программно осуществляемое по каналам связи. Это определение охватывает как удаленные атаки на информационную инфраструктуру и протоколы сети, так и удаленные атаки на операционные системы и приложения. Под инфрастуктурой сети понимается сложившаяся система организации между объектами сети и используемые в сети сервисные службы. А под операционными системами и приложениями – все программное обеспечение, работающее на удаленном компьютере, которое тем или иным образом обеспечивает сетевое взаимодействие.

Хотя информационная безопасность охватывает множество способов защиты, но основными из них являются следующие [3].

Целостность данных. Безопасная система должна защитить информацию от несанкционированного изменения и повреждения.

*Доступность данных***.** Система должна гарантировать, что несанкционированный пользователь не может помешать заданному доступу к данным.

Секретность и конфиденциальность. Система не должна позволять несанкционированным пользователям создавать копии данных во время их передачи по сети, а также анализировать их содержимое в том случае, если копии все-таки сделаны.

Авторизация. Меры информационной безопасности должны быть избирательными, учитывающими классификацию людей и ресурсов по различным категориям.

Аутентификация. Система должна позволять двум взаимодействующим между собой объектам проверить подлинность друг друга.

Запрещение повторного использования. Чтобы посторонние не могли перехватывать копии с целью их дальнейшего использования, система не должна обрабатывать копии повторно переданных пакетов данных.

Говоря об основных понятиях информационной безопасности, необходимо определиться и с людьми, так или иначе связанными с проблемами компьютерного взлома, так называемыми хакерами. Общественное мнение специалистов по отношении деятельности хакеров не однозначно, оно либо сугубо негативное (хакеры – преступники), либо достаточно позитивное (хакеры – «санитары леса»). В действительности, эта деятельность имеет как положительную сторону, так и сугубо отрицательную, и эти две стороны четко разграничены. В связи с этим некоторые авторы предлагают разделить всех профессионалов, связанных с информационной безопасностью, на хакеров (hackers) и кракеров (crackers). И те, и другие во многом занимаются решением одних и тех же задач – поиском уязвимости в вычислительных системах и осуществлением на них атак («взломом»).

Кракеры – специалисты, способные снять защиту от копирования с лицензионного программного обеспечения. В современном компьютерном андеграунде кракерами обычно называют взломщиков ПО, в то время как *хакерами* именуют людей, специализирующихся на взломе защиты отдельных компьютеров и распределенных систем.

Принципиальное различие между хакерами и кракерами состоит в целях, которые они преследуют. Основная цель хакера состоит в том, чтобы, исследуя вычислительную систему, обнаруживать слабые места (уязвимость) в ее системе безопасности и информиро-

вать пользователя и разработчиков системы с целью устранения найденных уязвимостей. Другая задача хакера – проанализировать существующую систему, сформулировать необходимые требования и условия повышения уровня ее защищенности. Задача кракера состоит в непосредственном осуществлении взлома системы с целью получения несанкционированного доступа к чужой информации для кражи, подмены или объявления факта взлома. Среди основных *целей кракеров* следует отметить следующие:

получить доступ к важной информации, закрытой по тем или иным соображениям от использования посторонними лицами;

получить доступ к ресурсам чужой системы (процессора, внешней памяти и т.п.), в этом случае владелец системы ничего не теряет, за исключением времени занятости процессора и части дискового пространства, но, возможно, и приобретает достаточно дорогое программное обеспечение;

нарушить работоспособность хоста, без реализации угрозы раскрытия (это может быть достаточно опасным, если хост обеспечивает бесперебойное обслуживание клиентов);

создать плацдарм для осуществления вышеназванных целей, но для атаки на другой компьютер с целью переадресовать корыстные цели на чужой компьютер;

отладить механизм атак на другие системы, используя Ваш компьютер в качестве пробного.

Мотивы кракеров низменны, но их состав неоднороден. Существует даже их классификация, в соответствии с которой кракеров разделяют на следующие категории:

вандалы – самые известные (благодаря распространению вирусов) и самая малочисленная часть кракеров (их основная цель – взломать систему для ее дальнейшего разрушения, это специалисты в написании вирусов и их разновидностей под названием «троянских коней», весь компьютерный мир ненавидит вандалов лютой ненавистью, эта стадия «кракерства» характерна для новичков и быстро проходит, если кракер продолжает совершенствоваться);

«шутники» – наиболее безобидная часть кракеров (основная цель «шутников» – известность, достигаемая путем взлома компьютерных систем и внедрения туда различных эффектов, выражающих их неудовлетворенное чувств юмора; к «шутникам» также можно отнести создателей вирусов с различными визуально-

звуковыми эффектами («музыкодрожание» или переворачивание экрана и т.п.); «шутники», как правило, не наносят существенного ущерба компьютерным системам и администраторам; все их действия – либо невинные шалости, либо рекламные акции профессионалов);

взломщики – профессиональные кракеры, пользующиеся почетом и уважением в этой среде (их основная задача – взлом компьютерной системы с серьезными целями, например с целью кражи или подмены хранящейся в системе информации; как правило, для того чтобы осуществить взлом, необходимо пройти три основных стадии):

исследование вычислительной системы с выявлением в ней изъянов (уязвимости);

разработка программной реализации атаки;

непосредственное осуществление атаки.

Настоящим профессионалом можно считать того кракера, который для достижения своей цели проходит все три стадии. В принципе, работа взломщиков – обычное воровство.

Однако в нашем отечестве, где находящееся у пользователей программное обеспечение в преобладающей части является пиратским, т.е. украденным не без помощи тех же взломщиков, отношение к ним не столь категорично.

В связи с этим, если не ограничиваться рассмотрением хакеров и кракеров с позиций распределенных систем, то следует отметить, что самая многочисленная категория кракеров занимается снятием защиты с коммерческих версий программных продуктов, изготовлением регистрационных ключей (registration key) для условно бесплатных программ (shareware) и т.п.

Говоря о хакерах, следует еще отметить, что в последнее время сформировался устойчивый *миф об их всемогуществе и полной незащищенности компьютерных систем*. Действительно, современные вычислительные системы общего назначения имеют серьезные проблемы с безопасностью. Но речь идет именно о системах общего назначения. Там же, где требуется обработка критической информации и обеспечение высшего уровня защиты (например, в военной области, атомной энергетике и т.п.), используются специализированные защищенные вычислительные системы, которые изолированы от сетей общего назначения физически и не допускают

несанкционированного удаленного доступа извне. В то же самое время любая уважающая себя организация, будь то ЦРУ, АНБ, НАСА, имеет свои www- или FTP-серверы, находящиеся в открытой сети и доступные всем, и кракеры в этом случае проникали именно в них.

Другим, еще более устойчивым мифом, является *миф о всеобщей беззащитности банковских систем*. Действительно, в отличие от вычислительных систем стратегического назначения банки вынуждены для обеспечения удобства и быстродействия работы с клиентами предоставлять им возможность удаленного доступа из сетей общего пользования к своим банковским вычислительным системам. Однако для связи в этом случае используются защищенные криптопротоколы и разнообразные системы сетевой защиты, и к тому же предоставление клиенту возможности удаленного доступа, отнюдь, не означает, что клиент может получить доступ непосредственно к внутренней банковской сети.

По мнению специалистов, зарубежные банковские вычислительные системы являются наиболее защищенными вслед за системами стратегического назначения. В обоих случаях речь идет о несанкционированном удаленном доступом извне. В том случае, если нанести ущерб системам вознамерится кракер из состава персонала защищенной системы, трудно судить об успехе его попыток. Известен, например, случай на Игналинской АЭС, когда местный системный программист внедрил в вычислительную систему программу («троянского коня»), которая едва не привела к аварии на станции. Как утверждают статистики, нарушение безопасности системы собственным персоналом составляет около 90 % от общего числа нарушений. Таким образом, даже критические вычислительные системы нельзя считать неуязвимыми, но реализовывать на них успешную удаленную атаку практически невозможно.

Аналогичный вывод можно сделать и по отношению к банковским системам. В качестве примера можно привести дело российского программиста Левина, вскрывшего City Bank и наделавшего много шума в прессе. Однако вряд ли ему удалось это сделать благодаря своим выдающимся программистским способностям. Наиболее убедительной является версия, что у него все же были сообщники в этом банке, которые предоставили ему входное имя и пароль. Неявным подтверждением этого факта является то, что он

не смог скрыть своих «следов» и довольно быстро был обнаружен правоохранительными органами.

Как утверждают некоторые авторы, ни одного подтвержденного факта целенаправленного взлома с помощью программных средств (а не с помощью подкупа и т.п.) указанных выше систем ни в России, ни за рубежом пока обнаружить не удалось.

11.4. Основные методы защиты от удаленных и локальных атак

Говоря об удаленных атаках, следует отметить, что защита от них взаимосвязана с методами доступа и использованными пользователем ресурсами глобальной сети. Сети являются общедоступными. Удаленный доступ к этим ресурсам может осуществляться анонимно любым неавторизированным пользователем. Примером неавторизированного доступа является подключение к www- или FTP-серверам. В этом случае, если трафик пользователя будет перехвачен, пройдет через сегмент атакующего, то последний не получит ничего, кроме общедоступной информации, т.е. отпадает забота о защите информации. Если же планируется авторизированный доступ к удаленным ресурсам, то следует обратить на эту проблему особое внимание.

Методы защиты связаны также с используемой пользователем операционной системой, имея при этом в виду: собирается ли пользователь разрешать удаленный доступ из сети к своим ресурсам. Если нет, то пользователь должен использовать чисто «клиентскую» ОС (например, Windows 98 или NT Workstation). Удаленный доступ к данной системе в принципе невозможен, что, безусловно, повышает ее безопасность (хотя и не гарантирует ее полностью). Естественно, все ограничения, связанные с безопасностью, ухудшают функциональность системы. В связи с этим существует такая аксиома безопасности: «Принципы доступности, удобства, быстродействия и функциональности вычислительной системы антагонистичны принципам ее безопасности. Чем более удобна, быстра и многофункциональна вычислительная система, тем она менее безопасна». Естественно, полная изоляция компьютера от глобальной сети путем отключения разъема или создания выделенной линии связи обеспечивает абсолютную безопасность

от удаленных атак, однако полностью исключает функциональные возможности сетей и поэтому бессмысленна. Основная же цель комплексной защиты информации – обеспечение максимальных функциональных возможностей при достаточной защищенности системы. Среди разнообразных мер по защите от удаленных атак наиболее простыми и дешевыми являются административные меры. Например, как можно защититься от анализа сетевого трафика злоумышленником, если известно, что с помощью программного прослушивания можно перехватить любую информацию, которой обмениваются удаленные пользователи, когда по каналу передаются нешифрованные сообщения? Также известно, что базовые прикладные протоколы удаленного доступа TELNET и FTP не предусматривают элементарную защиту передаваемых по сети идентификаторов (имен) и аутентификаторов (паролей).

Поэтому администраторы сетей могут запретить использовать эти базовые протоколы для предоставления авторизированного доступа к ресурсам своих систем. При необходимости можно рекомендовать средства защиты этих протоколов.

Определенную опасность представляет использование так называемого протокола ARP. Этот протокол осуществляет поиск и сопоставление IP-адреса с адресом конкретной локальной сети (например, Ethernet) и направление следования именно по этому адресу. Послав специально сформированный ARP-пакет, злоумышленник может заставить окружающие его компьютеры посылать информацию не на маршрутизатор, а на его компьютер, прослушивая таким образом весь проходящий через сеть трафик. Чтобы устранить эту неприятность, связанную с отсутствием у ОС каждого хоста необходимой информации о соответствующих IP- и Ethernet-адресах остальных хостов внутри данного сегмента сети, сетевой администратор создает статическую ARP-таблицу в виде файла, куда вносится необходимая информация об адресах. Данный файл устанавливается на каждый хост внутри сетевого сегмента, и, следовательно, у сетевой ОС отпадает необходимость использования удаленного ARP-поиска.

Известна также уязвимость адресной службы DNS, что позволяет кракеру получить глобальный контроль над соединениями путем навязывания ложного маршрута через хост кракера – ложный DNS-сервер. Это приводит к катастрофическим последствиям для

огромного числа пользователей. Защита от ложного DNS-сервера – достаточно сложная задача, однако и в этом случае могут быть предложены административные методы, которые могут предотвратить установление такого глобального контроля или защитить подобную удаленную систему. Разработаны административные меры от навязывания ложного маршрута, защиты от отказа в обслуживании и от других причин нарушения безопасности информации.

Признавая важность административных мер защиты от удаленных атак, тем не менее, следует считать, что основную роль играют все же программно-аппаратные методы защиты. Центральным элементом в комплексе программно-аппаратных методов является криптография. В течение многих лет криптография использовалась исключительно в военных целях с привлечением и внедрением фундаментальных научных исследований (достаточно вспомнить работы А. Тьюринга и их практическую реализацию в крупном вычислительном комплексе в Великобритании в период Второй мировой войны). Агентство национальной безопасности АНБ Соединенных Штатов Америки и его аналоги в бывшем Советском Союзе, Англии, Франции, Израиле и других странах затратили миллиарды долларов на разработку криптографических методов, пытаясь обеспечить безопасность собственных линий связи и одновременно – взломать все чужие. Как правило, работы этих ведомств по данной тематике носили секретный характер. В последние 20 – 30 лет наблюдается бурный рост несекретных академических исследований в области криптографии. Сегодня современная компьютерная криптография широко практикуется и за стенами военных ведомств, что, безусловно, связано с расширением сферы деятельности людей, в которых возникает потребность в криптографических методах защиты информации. Это научное направление имеет очень серьезное теоретическое (математическое, алгоритмическое) обоснование и связано с работами таких выдающихся ученых, как упоминавшийся выше Алан Тьюринг, Клод Шеннон, Давид Кан и др. В открытой печати уже появилось довольно много публикаций, учебников и солидных монографий по криптографии [11], [12], [13].

Конкретная реализация методов криптографии связана с разработкой аппаратных и программных средств, так, например, мейнфреймы фирмы IBM, начиная с 90-х годов оснащаются криптографическими процессорами, обеспечивающими шифрование и

дешифрование сообщений с минимальной дополнительной нагрузкой на центральный процессор. Эти спецпроцессоры могут обрабатывать большие объемы данных и обеспечивать высокий уровень защищенности вычислительных систем. Важную роль в реализации криптографических методов играет разработка генераторов «истинно случайных» чисел и другие исследования.

В качестве примера применения криптографических методов рассмотрим процедуру защиты IP-протокола в глобальной сети Интернет. Обеспечить безопасность глобальной сети Интернет особенно трудно, поскольку дейтаграммы, передающиеся от отправителя до конечного получателя, проходят через несколько промежуточных сетей и маршрутизаторов, не контролируемых ни отправителем, ни получателем. Таким образом, поскольку дейтаграммы могут быть перехвачены без ведома отправителя, их содержимому нельзя доверять. Например, рассмотрим сервер, который использует процедуру аутентификации источника для проверки того, что запросы поступают от авторизированных клиентов. Процедура аутентификации источника требует, чтобы сервер при получении каждой дейтаграммы проверял IP-адрес отправителя, и принимал запросы только от компьютеров, адреса которых перечислены в специальном списке. Данный вид аутентификации обеспечивает слабую защиту, поскольку ее можно легко обойти. В частности, один из промежуточных маршрутизаторов может контролировать трафик проходящих через него дейтаграмм и фиксировать IP-адреса авторизированных клиентов, которые могут быть перехвачены любым злоумышленником, контролирующим этот маршрутизатор. Затем этот злоумышленник может выступить в роли авторизированного клиента.

Группа IETF (Internet Engineering Task Forse) – инженерная группа, входящая в структуру архитектурного совета Интернет, разработала набор протоколов, которые обеспечивают безопасную связь в глобальной сети. Все вместе они называются семейством протоколов IPsec (IP security или защитным протоколом IP). В этих протоколах аутентификация и шифрование данных выполняются на уровне протокола IP.

Методы криптографии, применяемые при разработке разнообразных криптопротоколов, составляют основу программных методов защиты информации в сетях. В то же время они являются составной частью так называемой *методики Firewall*, являющейся

сейчас основой программно-аппаратных средств осуществления сетевой политики безопасности в IP-сетях и реализующих следующие функции.

Многоуровневая фильтрация сетевого трафика. Фильтрация обычно происходит на четырех уровнях OSI:

канальном (Ethernet);

сетевом (IP);

транспортном (TCP, UDP);

прикладном (FTP, TELNET, HTTP, SMTP и т.д.).

Фильтрация сетевого трафика является основной функцией системы Firewall и позволяет администратору безопасности сети централизованно осуществлять необходимую сетевую политику в выделенном сегменте IP-сети. Настроив для этого соответствующим образом Firewall, можно разрешить или запретить пользователям как доступ из внешней сети к соответствующим службам хостов или к хостам, находящимся в защищенном сегменте, так и доступ пользователей из внутренней сети к соответствующим ресурсам внешней сети.

Proxy – схема с дополнительной идентификацией и аутентификацией пользователей. Смысл proxy-схемы заключается в создании соединения с конечным адресатом через промежуточный сервер, называемый proxy-сервером (proxy – полномочный).

Создание приватных сетей с виртуальными IP-адресами. Если администратор безопасности считает целесообразным скрыть истинную топологию своей внутренней IP-сети, он может использовать proxy-сервер для отделения своей внутренней приватной сети со своими внутренними виртуальными IP-адресами, которые, очевидно, непригодны для внешней адресации. При этом proxy-сервер должен осуществлять связь с абонентами из внешней сети со своего настоящего IP-адреса. Эти же схемы применяются и в том случае, если для создания IP-сети выделено недостаточное количество IP-адресов. Основным аппаратным компонентом для реализации методики управления доступом к объединенной сети является специализированное устройство, называемое *брандмауэром*, ассоциируемое с термином Firewall (термин брандмауэр позаимствован из строительства, где он обозначает толстую несгораемую стену, благодаря которой секция строения становится непроницаемой для огня). Обычно брандмауэр устанавливается между внутренней

сетью организации и каналом, ведущим к внешним сетям (например, к глобальной сети Интернет), брандмауэры разделяют объединенную сеть на две области, которые неофициально называются внутренней и внешней. Хотя сама идея брандмауэра проста, ее реализация усложняется множеством факторов. Один из них – внутренняя сеть организации может иметь несколько внешних соединений. При этом необходимо сформировать периметр безопасности (security perimeter), установив брандмауэр на каждое внешнее соединение. Чтобы гарантировать эффективность периметра безопасности, во всех брандмауэрах должны использоваться одинаковые ограничения доступа. В противном случае злоумышленники могут обойти ограничения, наложенные одним брандмауэром, и зайти в объединенную сеть через другой.

Существует несколько способов реализации брандмауэров [10]. Выбор способа зависит от того, какое количество внешних каналов существует в организации. В большинстве случаев каждый барьер в брандмауэре реализуется на основе маршрутизатора, содержащего фильтр пакетов. Чтобы брандмауэр не замедлял работу сети, его аппаратное и программное обеспечение должно быть оптимизировано на решение конкретной задачи. Решению этой задачи способствует и тот факт, что в большинство коммерческих маршрутизаторов включен быстродействующий механизм фильтрации пакетов, который выполняет основную часть работы.

На практике, как правило, возникает необходимость создать безопасный брандмауэр, который предотвратит нежелательный доступ извне, и в то же время позволит пользователям внутренней сети получить доступ к внешним службам. При этом необходимо выработать специальный механизм безопасности. В общем случае организация может обеспечить доступ к внешним службам только через защищенный компьютер. Поэтому обычно с каждым брандмауэром связывают один защищенный компьютер и устанавливают на этом компьютере набор шлюзов уровня приложения. Для того чтобы такой компьютер мог служить в качестве безопасного канала связи, его степень защиты должна быть очень высока. Поэтому такой компьютер часто называют бастионным узлом. На бастионном узле запускаются службы, которые организация хочет сделать видимыми извне, а также proxy-серверы, которые позволяют внутренней сети получить доступ к внешним серверам. В брандмауэре

также может использоваться так называемая «тупиковая сеть», которая позволяет изолировать внешний трафик от внутреннего. К этой сети подключаются брандмауэры, а также бастионный узел.

Все брандмауэры можно разделить на три типа:

пакетные фильтры (packet filter);

серверы прикладного уровня (application gateways);

серверы уровня соединения (circuit gateways).

Все типы могут одновременно встретиться в одном брандмауэре.

Пакетные фильтры. Брандмауэры с пакетными фильтрами принимают решение о том, пропускать пакет или отбросить, просматривая IP-адреса, флажки или номера TCP-портов в заголовке этого пакета. IP-адрес и номер порта – информация сетевого и транспортного уровней соответственно, но пакетные фильтры используют и информацию прикладного уровня, так как все стандартные сервисы в TCP/IP ассоциируются с определенным номером порта.

Серверы прикладного уровня. Брандмауэры с серверами прикладного уровня используют серверы конкретных сервисов – TELNET, FTP и т.д. (proxy server), запускаемые на брандмауэре и пропускающие через себя весь трафик, относящийся к данному сервису. Таким образом, между клиентом и сервером образуются два соединения: от клиента до брандмауэра и от брандмауэра до места назначения.

Использование серверов прикладного уровня позволяет решить важную задачу – скрыть от внешних пользователей структуру локальной сети, включая информацию в заголовках почтовых пакетов или службы доменных имен (DNS). Другим положительным качеством является возможность аутентификации на пользовательском уровне.

При описании правил доступа используются такие параметры, как название сервиса, имя пользователя, допустимый временной диапазон использования сервиса, компьютеры, с которых можно пользоваться сервисом, схемы аутентификации. Серверы протоколов прикладного уровня позволяют обеспечить наиболее высокий уровень защиты – взаимодействие с внешним миром реализуется через небольшое число прикладных программ, полностью контролирующих весь входящий и выходящий трафик.

Серверы уровня соединения. Сервер уровня соединения представляет собой транслятор TCP-соединения. Пользователь образует соединение с определенным портом на брандмауэре, после чего последний производит соединение с местом назначения по другую сторону от брандмауэра. Во время сеанса этот транслятор копирует байты в обоих направлениях, действуя как провод.

Как правило, пункт назначения задается заранее, тогда как источников может быть много (соединение типа «один со многими»). Используя различные порты, можно создавать различные конфигурации. Такой тип сервера позволяет создавать транслятор для любого определенного пользователем сервиса, базирующегося на TCP, осуществлять контроль доступа к этому сервису, сбор статистики по его использованию.

Говоря о программных средствах защиты информации, необходимо отметить, что конечной целью атаки кракера является определенный компьютер, с конкретной реализацией сетевых протоколов, с конкретной определенной системой. В связи с этим необходимо коснуться защиты операционных систем. Среди типичных атак, которым могут быть подвергнуты любые ОС, можно указать следующие [6]:

кража пароля (подглядывание за несколькими пользователями, получение из файла, кража носителей и т.п.);

подбор пароля (перебор возможных вариантов, включая оптимизированный перебор);

копирование «жестких» дисков компьютера;

сбор «мусора»: если средство ОС позволяют восстанавливать ранее удаленные объекты, злоумышленник может получить доступ к удаленным объектам (удаленных другими пользователями), просмотрев содержимое их мусорных корзин;

превышение полномочий: используя ошибки в программном обеспечении или администрировании ОС, злоумышленник получает полномочия, превышающие те, которые предоставлены ему согласно действующей политике безопасности;

отказ в обслуживании (целью этой атаки является частичный или полный вывод ОС из строя, как правило, с помощью вирусов).

Самой распространенной ОС в глобальной сети Интернет является ОС Unix, основными протоколами, определяющими сети Интернет, являются протоколы TCP/IP, которые были разработаны

для ОС Unix. Не менее 90 % мощных Интернет-узлов работают под управлением этой ОС и различных ее диалектов. Основные концепции Unix разрабатывались в конце 60-х – начале 70-х годов прошлого столетия, когда не было никакой теории компьютерной безопасности, и никто не подозревал, о тех крупных неприятностях, которые возникнут по мере развития сетевых технологий.

Современные сетевые операционные системы оказываются в заведомо более выгодном положении, поскольку они разрабатывались с учетом ошибок Unix и современной ситуации с безопасностью сетей. Однако это вовсе не говорит об их большей безопасности.

За долгий срок жизни Unix исследователями написаны, а администраторами изучены сотни статей и книг относительно механизмов безопасности Unix и способов их нарушения. Все это позволяет предположить, что никаких сюрпризов Unix больше не преподнесет.

С новыми ОС ситуация прямо противоположная. И хотя в них заложены концепции, согласующиеся с современным состоянием теории безопасности, у них очень малый срок эксплуатации. Они активно исследуются хакерами и кракерами, и, несмотря на опыт Unix, начинают проходить тот же самый путь и совершать те же самые ошибки в обеспечении безопасности.

В дополнение к гл. 6 следует добавить несколько замечаний о структуре средств информационной безопасности ОС Unix и наиболее слабых ее местах. Как известно, изначально Unix была ориентирована на централизованные вычисления в системах коллективного пользования как многозадачная, многопользовательская ОС. Пользователи системы разделялись на группы, в зависимости от прав доступа (или привилегий):

суперпользователь (root), имеющий неограниченные права;

обычный пользователь, имеющий права в рамках своего идентификатора (UID, user ID) и членство в группе (GID, group ID) – права и ограничения устанавливаются для него суперпользователем.

По мере развития ОС и использования Unix-машин в качестве серверов в глобальных сетях среди обычных пользователей выделялись так называемые *специальные пользователи*. Они, как правило, имеют зарегистрированные имена (guest, bin, uucp и т.п.) и но-

мера UID и GID. Прав у этого пользователя еще меньше, чем у обычного. Их устанавливает суперпользователь для работы с конкретными приложениями. Одним из интересных примеров специального пользователя является анонимный пользователь FTP, который так и называется anonymous, или ftp.

И, наконец, есть категория так называемых *псевдопользователей*, не имеющих никаких прав и не идентифицируемых системой. Но они могут подключаться к системе с помощью так называемых *программ-демонов* (в современной терминологии серверов), в частности, используя средства электронной почты *e-mail*. От этого пользователя не требуется аутентификации, учет по нему также не ведется.

Именно две последние категории пользователей (особенно последняя) и являются причиной основных неприятностей в ОС Unix с точки зрения информационной безопасности. Среди основных причин уязвимости Unix принято считать наличие демонов; механизм SUID/SGID; излишнее доверие (поскольку в не столь давние времена создатели делали систему «под себя», не подозревая, насколько теснее и опаснее станет компьютерный мир через несколько лет); «люки».

Механизм SUID/SGID позволяет пользователю запускать некоторые программы с правами администратора системы, например для обеспечения возможности изменения собственного пароля, поскольку файл с паролями, разумеется, не доступен рядовым пользователям.

Также слабым местом Unix-систем являются «люки». Люком, или «черным входом» (backdoor), часто называют оставленную разработчиком недокументированную возможность взаимодействия с системой (чаще всего – входа в нее), например известный только разработчику универсальный «пароль». Люки оставляют в конечных программах вследствие ошибки, не убрав отладочный код, или вследствие необходимости продолжения отладки уже в реальной системе из-за ее высокой сложности, или же из корыстных интересов. Люки – любимый путь в удаленную систему не только у хакеров, но и у журналистов, и режиссеров вместе с подбором «главного» пароля перебором за минуту до взрыва, но в отличие от последнего способа люки реально существуют. Классический пример люка – это, конечно, отладочный режим в sendmail.

Учитывая динамику развития ОС Unix в настоящее время, можно сказать, что она является наиболее мощной и надежной, в том числе и с точки информационной безопасности системы.

На рынке достаточно много предложений средств защиты Интернет, однако по ряду параметров ни одно из них не может быть признано адекватным задачам защиты информации именно для Интернет. Например, достаточно криптостойкой и замечательной по своей идее является распространенная система PGP (Pritty good privacy). Однако, поскольку PGP обеспечивает шифрование файлов, она применима только там, где можно обойтись файловым обменом. Защитить, например, приложения «on-line» при помощи PGP затруднительно. Кроме того, уровень иерархии управления защиты PGP слишком высок: эту систему можно отнести к прикладному или представительскому уровням модели OSI. Стыковка защиты PGP с другими прикладными системами потребует также определенных усилий, если, конечно, вообще окажется осуществимой. Альтернативу таким «высокоуровневым» системам защиты среди традиционных решений составляют устройства защиты канального и физического уровня – скремблеры и канальные шифраторы. Они «невидимы» с прикладного уровня и в этом смысле совместимы со всеми приложениями. Однако такие системы имеют ограниченную совместимость с различным каналообразующим оборудованием и физическими средами передачи данных. Это, как правило, не сетевые устройства, способные распознавать топологию сети и обеспечить связь из конца в конец через многие промежуточные узлы, а «двухточечные» системы, работающие на концах защищаемой линии и поэтому вносящие значительную аппаратную избыточность. И, конечно же, на таких устройствах невозможно построить систему защиты в рамках такой сети, как Интернет, уже хотя бы потому, что невозможно обеспечить их повсеместное распространение (вследствие высокой цены) и всеобщую аппаратную совместимость.

В заключение этого краткого обсуждения методов защиты информации следует отметить, что люди представляют собой наиболее уязвимое звено в любой системе безопасности. Служащий фирмы либо по злому умыслу, либо по неосторожности, либо, не зная принятой в организации стратегии, может поставить под угрозу самую современную систему безопасности. В изучении методов

защиты информации сложилось даже целое направление – социальная инженерия, связанная со злоупотреблением доверия пользователей, например, как одним из наиболее эффективных методов получить информацию у ничего не подозревающих людей, особенно в больших организациях, где многие пользователи не знают персонал своих компьютерных подразделений «в лицо», общаясь, в основном, по телефону. По определению самих хакеров «социальная инженерия» – термин, используемый взломщиками и хакерами для обозначения несанкционированного доступа другим способом, чем взлом программного обеспечения; цель – обмануть людей для получения паролей к системе или иной информации, которая поможет нарушить безопасность системы. Классическое мошенничество включает звонки по телефону, электронную почту, разговоры по Интернет в «реальном времени», обыкновенную почту, личные встречи и т.п.

11.5. Компьютерные вирусы

Проблема «вирусов» и «вирусной безопасности» возникла достаточно давно. Первые исследования саморазмножающихся искусственных технических и программных конструкций проводились в середине прошлого столетия в работах фон Неймана, Винера и других ученых. Было дано определение и проведен математический анализ конечных автоматов, в том числе и самовоспроизводящихся. Термин «компьютерный вирус» появился позднее – официально считается, что его впервые употребил сотрудник Лехайского университета (США) Фред Коэн в 1984 г. на Седьмой конференции по безопасности информации, проходившей в США. Идеи вирусов были изложены широкой публике еще в 1983 г. известным разработчиком ОС Unix Кэном Томпсоном в одной из своих лекций.

Одной из самых известных практических реализаций чисто теоретических работ фон Неймана и других известных ученых, явилась программа Worm («червь»), созданная осенью 1988 г. студентом выпускного курса Корнельского университета Робертом Морисом, который занимался в Bell Laboratories программным обеспечением безопасности Unix. Запущенный на сетевой машине «червь» искал в сети Интернет машины с серверами и использовал их для воссоздания себя в большом количестве копий. Такое дейст-

вие «червя» стало возможным в результате использования ошибки в программе («демоне») Unix fingerd. Вирус распространялся с поразительной скоростью и появлялся в самых различных районах США. Через пять часов было поражено пять систем, через двое суток – шесть тысяч. По самым скромным оценкам вирус Мориса стоил свыше 8 млн ч потери доступа и свыше миллиона часов прямых потерь на восстановление работоспособности систем. Общая стоимость этих затрат оценивается в 98 млн дол. Ущерб был бы еще большим, если бы вирус изначально создавался с разрушительными целями.

Этот крупнейший инцидент в области компьютерной безопасности доказал (не теоретически, а практически) возможность создания саморепродуцирующихся программ, дал толчок к появлению целой отрасли компьютерной безопасности – компьютерной вирусологии, а также выявил необходимость разработчиков Unix более серьезно заняться безопасностью этой ОС. К тому времени уже существовали единичные вирусы и на персональных компьютерах – саморепродуцирующиеся в пределах одного компьютера (видимо, поэтому сетевые вирусы стали называться «червями»).

Так что же такое компьютерный вирус? По определению, данному одним из известных отечественных специалистов Евгением Касперским, компьютерным вирусом называется программа, которая может создавать свои копии и внедряться в файлы и системные области компьютера, вычислительной сети и т.п. При этом копии сохраняют способность дальнейшего распространения. Другими словами, *компьютерный вирус* – небольшая программа (средний размер – 700 байт), написанная на языке Assembler и выполняющая разрушительные для ОС действия. Следует отметить, что такие программы как «бомбы» и «троянские кони» также приводят к неприятностям в системах, но отличаются от вирусов, так как не обладают свойством саморазмножения.

Название «вирус» распространилось ввиду явного сходства с биологическим прототипом. Суть воздействия биологического вируса сводится к нарушению информации, содержащейся в генетическом коде клетки. Посредством небольшого изменения фрагмента ДНК и РНК он захватывает управление жизненным процессом клетки. Таким образом, вирус обеспечивает себе возможность сво-

бодно и неограниченно размножаться. Это часто приводит к трагическим последствиям.

Если компьютерную систему сопоставить с живым организмом, а отдельные программы – с клетками, то получим полную аналогию. Компьютерный вирус разрушает информацию, содержащуюся в коде программы. Он перехватывает контроль над компьютерной системой путем замены небольшого фрагмента программы, что позволяет ему неограниченно размножать свой код. Так же, как и биологический аналог, компьютерные вирусы:

представляют опасность для той системы, на которой они паразитируют;

быстро размножаются, легко распространяются на большие расстояния;

проявляют себя не сразу;

имеют «латентный период», во время которого вирус продолжает распространяться в компьютерной системе;

играют важную роль в борьбе с «заболеваниями».

Биологическая аналогия оказывается настолько глубокой, что в литературе, посвященной компьютерным вирусам, широко используются и другие медицинские термины: «заболевание», «вакцина», «лечение», «карантин» и др., что иногда приводит к недоразумениям, когда забывается, что компьютерный вирус является обычной программой для компьютерной системы, которая имеет своего создателя.

Вирусы можно разделить на классы по следующим признакам:

по среде обитания вируса;

по способу заражения среды обитания;

по деструктивным возможностям.

По среде обитания различают, прежде всего, *сетевые вирусы*, или *вирусы-черви* (*worm*), которые распространяются в компьютерной сети. Проникая в память компьютера, они вычисляют сетевые адреса других машин и по этим адресам рассылают свои копии.

Файловые вирусы являются наиболее распространенным типом и обладают наибольшей инфицирующей способностью. Объектом поражения файловых вирусов являются исполняемые файлы, драйверы устройств и файлы ОС. По способу заражения файловые вирусы делятся на *резидентные* и *нерезидентные.*

Нерезидентный файловый вирус при запуске пораженной программы ищет первую «жертву» – незараженный файл в текущей директории, и дописывает к ней свое тело, а затем передает управление запущенной программе. Нерезидентные вирусы не заражают память компьютера и сохраняют активность ограниченное время.

Резидентные вирусы находятся в памяти компьютера, оставляя в оперативной памяти свою резидентную часть, которая перехватывает обращение ОС к объектам заражения и внедряется в них. Резидентные вирусы находятся в памяти и остаются активными вплоть до выключения компьютера или его перезагрузки.

Загрузочные вирусы внедряются в загрузочный сектор системного диска, проникая в компьютер при загрузке зараженной дискеты. При идентифицировании диска вирус в большинстве случаев переносит оригинальный boot-сектор в какой-либо другой сектор диска, а сам записывается на его место. В результате при загрузке с зараженного диска вместо настоящего boot-сектора будет выполнен программный код вируса, который при первой возможности делает свое «черное дело». В настоящее время этот вид вирусов практически обречен, так как практически все машины имеют защиту boot-сектора.

Вирусы всех типов могут распространяться по сети. По своим деструктивным возможностям «троянский» компонент вируса обычно разделяют на:

безвредные вирусы, никак не влияющие на работу компьютера, кроме изменения свободной памяти на диске в результате своего размножения;

неопасные вирусы, влияние которых ограничивается уменьшением объема свободной памяти на диске и графическими, звуковыми и прочими эффектами, к которым относится, например, выдача букв или проигрывание какой-нибудь мелодии в определенное время;

опасные вирусы, которые могут привести к серьезным сбоям в работе компьютера;

очень опасные вирусы, которые могут привести к потере программ; уничтожить данные; стереть необходимую для работы компьютера информацию, записанную в системных областях памяти; и даже способствовать ускоренному износу движущихся частей диска.

Вирусы-«черви» (*worm*) – вирусы, которые распространяются в компьютерной сети и, так же как и вирусы-«спутники», не изменяют файлы или секторы на дисках. Они проникают в память компьютера из компьютерной сети, вычисляют сетевые адреса других компьютеров и рассылают по этим адресам свои копии. Такие вирусы иногда создают рабочие файлы на дисках системы, но могут вообще не обращаться к ресурсам компьютера (за исключением оперативной памяти).

Большинство вопросов связано с термином «полиморфный вирус». Этот вид компьютерных вирусов представляется на сегодняшний день наиболее опасным. *Полиморфные вирусы* – вирусы, модифицирующие свой код в зараженных программах таким образом, что два экземпляра одного и того же вируса могут не совпадать ни в одном бите. Такие вирусы не только шифруют свой код, но и содержат код генерации шифровщика и расшифровщика, что отличает их от обычных шифровальных вирусов, которые также могут шифровать участки своего кода, но имеют при этом постоянный код шифровальщика и расшифровщика. Полиморфные вирусы – вирусы с самомодифицирующимися расшифровщиками. Цель такого шифрования: имея зараженный и оригинальный файлы, вы все равно не сможете проанализировать его код с помощью обычного дизассемблирования. Этот код зашифрован и представляет собой бессмысленный набор команд. Расшифровка производится самим вирусом уже непосредственно во время выполнения. При этом возможны варианты: он может расшифровать себя всего сразу, а может выполнять такую расшифровку «по ходу дела», может вновь шифровать уже отработавшие участки. Все это делается с целью затруднения анализа кода.

Отметим еще *макровирусы*. Это особая разновидность вирусов, которые поражают документы в прикладных программах, имеющие расширение .doc, например документы, созданные текстовым процессором MS Word и выполняющие макрокоманды. Если открыть файл документа в окне, происходит заражение.

Абсолютных гарантий антивирусной безопасности не имеется, даже при наличии самых наилучших антивирусных программ. Однако путем соблюдения определенных правил профилактики (так называемой компьютерной гигиены), можно снизить до минимума риск заражения компьютеров.

Необходимо регулярно делать резервные копии файлов, с которыми ведется работа, на внешний носитель.

Следует покупать дистрибутивные копии программного обеспечения только у официальных продавцов.

Не следует запускать непроверенные антивирусные программы, полученные из сомнительных источников.

При лечении дисков следует использовать заведомо «чистую» операционную систему.

Необходимо иметь в виду, что очень часто вирусы переносятся с игровыми программами, с которыми следует быть предельно осторожным. В заключение следует отметить, что, кроме вирусов, существует другой вид программ, представляющих опасность для вычислительных систем, о которых ранее упоминалось. Это так называемые «троянские» программы. Такие программы не способны самостоятельно размножаться, и их распространение основано целиком на добровольном копировании. При запуске такой программы она, выполняя внешне безобидные действия, одновременно портит данные в компьютере. «Троянские программы» распространяются значительно медленнее, чем вирусы, поскольку, уничтожив систему, они погибают сами. Как правило, их маскируют под игровые программы или широко известные пакеты.

11.6. Криптографические методы защиты информации

Поскольку в основе всех автоматизированных сетевых и компьютерных систем безопасности находится криптография, пользователю любого уровня полезно иметь хотя бы общее представление об этом направлении развития вычислительных систем.

Слово «криптография» греческого происхождения и означает тайнопись, в современной терминологии – шифрование, которое заключается в преобразовании открытого текста или данных в нечитаемую форму при помощи обратимых математических операций.

До изобретения в 70-х годах XIX в. шифрования с так называемым открытым ключом традиционное шифрование (иногда называемое шифрование с обычным ключом) было единственным типом шифрования. Этот тип шифрования использовался для секретного взаимодействия очень многими людьми и группами людей, начиная с Юлия Цезаря и заканчивая немецкими подводными лод-

ками, а также современными дипломатами, военными, бизнесменами и т.п. Традиционное шифрование до сих пор остается самым популярным, используя алгоритм, при котором шифрование и дешифрование осуществляется при помощи одного и того же ключа (метода преобразования текста).

Традиционную схему шифрования образуют пять составляющих.

Открытый текст – исходное сообщение или данные, которые подаются на вход алгоритма.

Алгоритм шифрования – различные способы преобразования текста.

Секретный ключ подается также на вход алгоритма шифрования наряду с открытым текстом. Конкретные операции замены и перестановки, выполняемые алгоритмом, зависят от ключа.

Зашифрованный текст – искаженное сообщение, формируемое на выходе алгоритма. Зашифрованный текст представляет собой функцию открытого текста и секретного ключа. Если закодировать одно и то же сообщение с помощью двух разных ключей, получим два разных варианта зашифрованного текста.

Алгоритм дешифрования – алгоритм шифрования, работающий в реверсивном режиме. Он принимает на вход зашифрованный текст и секретный ключ, а на выходе генерирует оригинальный открытый текст.

Для обеспечения безопасности традиционного шифрования необходимо выполнение двух условий:

нужен надежный алгоритм шифрования, секретный ключ которого не должен быть доступен злоумышленнику;

отправитель и получатель должны получать копии секретного ключа безопасным образом и обеспечить надежное его хранение.

Существует два основных способа атаки на традиционную схему шифрования, первый из которых называется криптоанализом, он опирается на природу алгоритма, а также на определенные сведения об общих характеристиках открытого текста, включая примеры перехваченных пар открытого и зашифрованного текстов. Цель заключается в выявлении ключа шифрования. Второй метод называется «методом грубой силы» или решением задачи «в лоб». Он включает полный перебор всех возможных вариантов ключа к зашифрованному сообщению, пока не будет получен осмысленный

вариант открытого текста. Это требует зачастую вычислительных систем высокой производительности и зависит от размерности ключа шифрования, которая может изменяться в широких пределах.

Существует ряд стандартов шифрования. Так, Национальный институт стандартов и технологий США (NIST) принял следующие стандарты:

DES (Data Encryption Standard – стандарт шифрования данных), в котором открытый текст разбивается на блоки по 64 бит, каждый из которых кодируется с помощью 56-разрядного ключа;

тройной алгоритм TDEA (Tryple DEA), представляющий троекратное шифрование методом DES, разработанный в связи с потенциальной уязвимостью DES, принят как стандарт ANSI для использования в финансовых приложениях при трех различных ключах, эффективная длина ключа составляет 68 бит;

алгоритм шифрования AES (Advanced Encryption Standard – передовой стандарт шифрования), был разработан как альтернатива TDEA, который при очень высокой надежности и эффективности работал очень медленно и имел очень короткие блоки обработки (что взаимосвязано).

Шифрование с открытым ключом впервые было предложено в 1976 г. Диффи (Diffie) и Хеллманом (Hellman) и представляет прорыв в криптографии, первый за последнюю тысячу лет. Эта разновидность криптографической системы, в которой шифрование и дешифрование осуществляется при помощи двух различных ключей, один из которых называется открытым, а второй закрытым, т.е. шифрование становится асимметричным. В основе алгоритмов шифрования открытым ключом лежат математические функции, а не простые операции с последовательностью битов, характерные для симметричного шифрования.

В схему шифрования с открытым ключом входит шесть составляющих:

открытый текст – исходное сообщение или данные, которые подаются на вход алгоритма;

алгоритм шифрования, представляющий различные способы преобразования текста;

открытые и закрытые ключи, которые выбирают таким образом, что один применяется для шифрования, а другой для дешифрова-

ния (конкретные преобразования, осуществляемые с открытым текстом, зависят от используемого открытого или закрытого ключей);

зашифрованный текст – искаженное сообщение, формируемое на выходе алгоритма (зашифрованный текст представляет собой функцию открытого текста и ключа, если зашифровать одно и тоже сообщение с помощью двух различных ключей, получим два различных варианта зашифрованного текста);

алгоритм дешифрования (включается, когда на его вход поступает зашифрованный текст и второй ключ пары, а на выходе генерируется оригинальный текст).

Процесс работает независимо от того, в каком порядке действует пара ключей. Открытый ключ публикуется для использования всеми желающими, тогда как закрытый ключ известен только владельцу. Одним из основных достоинств этого метода является то, что вычислительными методами трудно определить закрытый ключ по открытому.

Очень удачной аналогией этого способа кодирования является почтовый ящик. Шифрование открытым ключом аналогично опусканию письма в почтовый ящик – может сделать кто угодно, просто открыв паз и опустив письмо в почтовый ящик. Расшифрование с закрытым ключом при этом подобно извлечению почты из почтового ящика. Открыть его гораздо сложнее. Обычно если у вас есть ключи от почтового ящика, извлечь письмо не трудно.

Один из наиболее популярных алгоритмов при шифровании открытым ключом является алгоритм RSA (Rivest – Shamir – Adleman), предложенный в 1977 г. сотрудником Массачусетского технологического института. В этом алгоритме открытый и зашифрованный тексты рассматриваются как целые числа в диапазоне от 0 до $n - 1$. Для шифрования в сети используются арифметические операции деления по модулю. Алгоритм шифрования основан на сложности разложения большого числа на множители.

Однако при всех достоинствах шифрования открытым ключом не следует считать, что он является универсальной технологией, с появлением которой традиционное шифрование можно считать устаревшим. Современные схемы шифрования открытым ключом требуют очень больших объемов вычислений, что вряд ли позволит отказаться в обозримом будущем от традиционных методов шиф-

рования. К тому же распространение ключей в данном методе шифрования, отнюдь, не представляет тривиальную задачу. Следует также отметить, что защита от криптоанализа при шифровании открытым ключом не всегда лучше, чем у традиционного шифрования. В связи с этим оба эти метода применяются на практике, дополняя друг друга.

Важным криптографическим дополнением, подтверждающим достоверность передаваемой зашифрованной информации, является использование так называемой цифровой подписи, которая, с одной стороны, обеспечивает аутентификацию пользователей, а с другой стороны – исключает отказ посылающего от своего сообщения.

Следует отметить, что подпись от руки издавна пользуется для доказательства авторских прав или согласия с документом. Среди наиболее важных моментов подписи следующие:

подпись достоверна, убеждает получателя, что человек, подписавший документ, сделал это сознательно;

подпись не поддельна, она доказывает, что именно указанный человек подписал документ;

подпись невозможно использовать повторно, она часть документа, ее невозможно нанести на другой документ;

подписанный документ изменить невозможно;

от подписи нельзя отречься.

Хотя все эти утверждения не бесспорны, однако действия мошенников в традиционно подписываемых документах затруднены, и они рискуют быть разоблаченными.

Однако реализация электронной подписи и передача ее в сетях требует специальной защиты, так как ситуация оказывается гораздо сложнее. Во-первых, компьютерные файлы легко копируются. Даже если подпись человека – графическое изображение, подписи от руки подделать нелегко, можно без труда «вырезать» подлинную подпись из этого документа и вставить ее в другой. Таким образом, просто наличие в документе такой подписи ничего не означает. Во-вторых, компьютерные файлы легко изменить уже после подписания документа, не оставив ни малейшего следа изменения.

В связи с этим механизм цифровой подписи, реализуемый криптографическими методами, состоит из двух процессов:

формирование подписи блока данных – при передаче блока данных используется не только шифрование открытым ключом, но

также еще один алгоритм, называемый защитной функцией хэширования, которая определяется из передаваемого сообщения;

проверка подписи в принятом блоке данных.

Любое изменение сообщения злоумышленником приводит к изменению хэш-кода и недостоверности подписи при дешифровке. Фактически к сообщению добавляются данные, играющие роль подписи, поскольку они шифруются закрытым ключом отправляющего сообщение, что является гарантией подлинности и целостности документа.

Одним из самых ранних примеров использования цифровой подписи было упрощение проверки соблюдения договоров о ядерных испытаниях. Соединенные Штаты, Советский Союз разрешали друг другу разместить за границей сейсмографы для мониторинга ядерных испытаний. Проблема заключалась в том, что каждая сторона хотела быть уверенной в том, что страна, в которой размещены приборы, не подделывает их показаний. В свою очередь, страна, в которой размещались сейсмографы, искала гарантий, что приборы посылают только ту информацию, которая нужна для мониторинга и испытаний.

Эта проблема была решена с помощью цифровых подписей.

Страна, на территории которой стоял сейсмограф, может читать, но не изменять данные сейсмографа, а наблюдающая сторона знает, что данные не подделываются. Таким образом, комбинируя цифровые подписи и криптографию открытым ключом можно создать протокол, сочетающий надежное шифрование с достоверностью цифровых подписей.

Еще один вопрос, который неизбежно возникает при внедрении криптографических устройств, – вопрос о месте их размещения. Имеется два варианта решения этого вопроса: шифрование в линиях и сквозное шифрование.

При шифровании в линиях каждая уязвимая линия оборудуется на обоих концах шифрующими устройствами. Таким образом, может быть защищен весь трафик во всех линиях связи, хотя в большой сети для этого потребуется очень много таких устройств.

Один из основных недостатков такого подхода связан с тем, что на каждом промежуточном коммутаторе виртуального канала сообщение должно быть дешифровано и зашифровано заново с тем, чтобы определить адрес необходимого направления пакета. Таким

образом, сообщение оказывается уязвимым на каждом коммутаторе, поскольку в общественных сетях с коммутацией пакетов пользователь не может контролировать безопасность каждого узла. Кроме того, шифрование в линиях при существующих на сегодня скоростях передачи данных находится на пределе технических возможностей, что ограничивает применение данного варианта шифрования.

При сквозном шифровании криптографический процесс выполняется на двух оконечных системах. В зашифрованном виде данные пересылаются по сети без каких-либо изменений, вплоть до хоста, которому предназначаются эти данные. Такой подход должен вроде бы защищать от атак на сетевые коммутаторы, однако у данного подхода также есть слабое место. Для того, чтобы коммутаторы могли направлять пакеты по нужному адресу, заголовок письма не должен быть зашифрован. Таким образом, при сквозном шифровании пользовательские данные надежно защищены, однако маршрут данных не защищен, так как заголовок пакетов не шифруется.

Для повышения уровня защиты возникает необходимость совместного использования обоих методов – сквозного шифрования с включением элементов шифрования в линиях. В заключение следует сказать, что шифрование, состоящее в сокрытии содержания сообщения путем приведения его в нечитаемый вид, является наиболее важным автоматизированным средством обеспечения сетевой безопасности.

Традиционное шифрование и шифрование с открытым ключом часто комбинируются для предоставления услуг, связанных с обеспечением безопасности. Передаваемые данные шифруются традиционными методами, часто с помощью одноразового сеансового ключа. Сеансовый ключ может передаваться доверенным центром распространения ключей в зашифрованном, по алгоритму шифрования с открытым ключом, виде.

Шифрование с открытым ключом также может использоваться для создания цифровых подписей с целью аутентификации источников сообщений.

11.7. Бизнес в Интернете

В конце 1999 г. сразу два автомобильных гиганта Ford и General Motors объявили о своем намерении перевести большую часть своих коммерческих операций во Всемирную паутину и объединить поставщиков, деловых партнеров и покупателей во всем мире на виртуальных рынках. Это были первые примеры того, как крупные компании собираются воспользоваться Интернетом, чтобы оказаться в центре новой электронной коммерческой системы, способной изменять сам способ ведения бизнеса. При этом появляется возможность преобразовать всю традиционную цепочку поставки, соединяющую несколько последовательных операций. Взамен создается некоторый треугольник, в котором Интернет помогает образовать динамическое информационное пространство между поставщиком и потребителем. Интернет-коммерция не только позволяет получить огромный выигрыш в производительности, но также обеспечивает непосредственное сотрудничество, повышая гибкость и ответственность всех партнеров. А когда использовать web-системы начинают крупные фирмы, на работу через Интернет начинают переходить десятки тысяч деловых партнеров. Для поддержки web-коммерции необходимо применение технологий интранета и экстранета. Соответствующая сетевая инфраструктура должна поддерживать три типа деловой активности.

Внутрикорпоративный бизнес. В основе внутренней деловой активности лежат технологии интранета. Интранет должен охватывать не только сотрудников центрального офиса, но также филиалы и удаленных пользователей. Ключевое требование состоит в предоставлении удаленным сотрудникам того же уровня обслуживания, что и локальным сотрудникам и в одновременном обеспечении того же уровня безопасности, как во внутренней сетевой инфраструктуре.

Бизнес между производителями. Большинство решений, поддерживающих операции между производителями, построены по технологии безопасного экстранета. В большинстве случаев эту функцию выполняет корпоративный брандмауэр.

Бизнес между производителем и покупателем. Операции между производителем и потребителем представляют собой наиболее заметный тип электронной коммерции (для потребителя), знакомый среднему web-пользователю. Этот тип коммерции основан на ис-

пользовании корпоративного web-сайта, с которым соединяются потребители для совершения покупок и получения поддержки.

Финансовые операции в сети (или, как их принято называть в данном контексте, транзакции) между крупными потребителями и поставщиками уже существуют. Так, успешно используются такие эффективные платежные системы, как EFT (Electronic Funds Transfer – электронный перевод денежных средств), EDI (Electronic Data Interchange – электронный обмен данными). Для установления финансовых отношений существуют готовые стандартные методы проверки кредитоспособности и других параметров транзакций, мало чем отличающихся от методов проверки неэлектронных транзакций, однако транзакции между случайным продавцом и покупателем, не имевших дело друг с другом, ставят новые проблемы.

Интернет представляет собой огромный потенциальный рынок. Число пользователей и компаний, имеющих доступ в Интернет, стремительно растет и все эти пользователи обладают графическими браузерами. Его потенциальные коммерческие возможности очевидны. Сегодня практически вся коммерческая реклама содержит ссылки на web-сайты. Такие ссылки содержатся на упаковке товаров. Однако Интернет-коммерция отличается от традиционной коммерции. Такие достоинства Интернета, как общедоступность, популярность и скорость обслуживания, оборачиваются серьезной проблемой, связанной с потенциальными угрозами, которые обсуждались в предыдущих разделах. Такие крупные фирмы, как AT&T, IBM и Microsoft, на собственном опыте убедились, как, столкнувшись с феноменом всемирной паутины, тщательно выверенные рыночные планы могут стать бесполезными за очень короткое время. И, с другой стороны, жесткая анонимность и недоступность транзакций в финансовой сфере обладает определенной противоречивостью. Отслеживание транзакций бывает необходимо для борьбы с уклонением от налогов, отмыванием преступных денег, выкупом заложников, а также для борьбы с финансированием террористической деятельности.

В реализации Интернет-коммерции существенным являются новые технологические успехи в области связи, шифрования и платежных систем. Наиболее универсальное решение проблемы защиты транзакций заключается в использовании протокола, функционирующего между протоколом транспортного уровня (TCP) и при-

ложением. Наиболее известным применением такого протокола является протокол SSL (Secure Sockets Layer – слой защитных сокетов) и основанный на нем Интернет-стандарт, известный как TLS (Transport Layer Security – безопасность транспортного уровня). При этом возможны два варианта реализации. Для полной универсальности протоколов SSL (стандарт TLS) может быть реализован как часть низлежащего стека протоколов и, таким образом, быть прозрачным для приложений. Альтернативный подход заключается во внедрении SSL в конкретные пакеты. Например, web-браузер Netscape и Microsoft поставляются с встроенной поддержкой SSL, и большая часть web-серверов также поддерживает этот протокол. Работа протокола SSL прозрачна для пользователя. Механизм безопасности реализован поверх базовой службы TCP/IP.

Этот протокол обеспечивает защиту транзакций с помощью различных алгоритмов шифрования как открытым ключом на начальном этапе клиента и сервера (во время процедуры так называемого рукопожатия), так и шифрования симметричным ключом пересылаемых данных.

Очень важной задачей использования Интернета, взаимосвязанной с проблемой защиты транзакций, является задача создания эффективных электронных платежных систем.

Для электронной коммерции было предложено много электронных платежных систем. Среди наиболее распространенных систем является система SET (Secure Electronic Transaction – безопасная электронная транзакция), предложенная компаниями MasterCard и Visa для операции с банковскими картами в Интернете. Эта система позволяет в режиме подключения (on-line) к сети выполнять стандартные банковские операции. Другая система более привлекательная в ряде отношений (однако менее распространенная по определенным причинам) – так называемая система «электронных денег», которую предполагается реализовать в проекте Digit Cash, разработанная Дэвидом Чаумом.

Модель электронной торговли с помощью Master Card и Visa можно представить в виде следующей схемы.

1. Посещение магазина и изучение продаваемых товаров – пользователь ищет интересующий его товар при помощи инструментальных средств (например, браузера), подобно тому, как сегодня используется реклама и телефон.

2. Выбор продавца и товара – с помощью полученной информации владелец банковской карточки выбирает нужный ему товар и продавца.

3. Заказ и переговоры – владелец банковской карточки заполняет электронный бланк заказа и просматривает его для проверки заказанных товаров и цен на них. В этот момент на основании заказанных товаров и других обстоятельств обсуждаются скидки и другие параметры оплаты и стоимости.

4. Выбор платежного средства – владелец банковской карты и продавец договариваются о средствах платежа.

5. Авторизация и передача платежа – владелец банковской карты инициирует процедуру оплаты и с этого момента в дело вступает система SET.

6. Подтверждение и отчет – получив от владельца банковской карты заказ на товар, продавец запрашивает у системы SET авторизацию. Кроме того, продавец посылает владельцу банковской карты подтверждение и отчет о состоянии заказа.

7. Доставка товара – получив авторизацию, продавец отправляет владельцу банковской карты заказанные им товары.

8. Покрытие расходов продавца – отправив товар заказчику, продавец обращается к системе SET, инициируя запрос на возмещение расходов.

В системе SET для защиты конфиденциальности финансовой информации используются как методы шифрования симметричным ключом, так и методы шифрования открытым ключом. Представляется аутентификация с использованием цифровых подписей и гарантии с помощью алгоритмов кэширования.

Как следует из схемы взаимодействия между продавцом и покупателем, кроме этих двух участников существует третья сторона – финансовое учреждение (некоторый посредник), как у покупателя, так и у продавца, которая и осуществляет необходимые финансовые операции. При этом покупатель удален от своих финансовых средств, т.е. наличных денег, что не всегда удобно.

Предложенная Дэвидом Чаумом электронная платежная система исключает недостатки системы SET. Оплата в этой системе осуществляется в автономном режиме, пользователю предоставляется возможность совершить покупки без установки соединения с третьей стороной, представляющей пользователя или продавца для

авторизации или ратификации. В идеале электронные деньги должны обладать рядом качеств, такими, как конфиденциальность, переносимость, делимость и т.п.

В этой системе у каждого пользователя электронных денег есть счет в финансовом учреждении, поддерживающем эту систему. На жестком диске рабочей станции каждого покупателя также есть «бумажник» Digit Cash, содержащий маркеры (электронные «монетки»), вычитаемые из суммы на его счету. Эти маркеры представляют собой пакеты данных, создаваемые алгоритмом обслуживания цифровых денег. Использование электронных денег происходит по следующей схеме: после того как пользователь запускает свою программу электронных денег, она работает на его персональном компьютере в фоновом режиме. В небольшом окне можно видеть, сколько электронных «монеток» хранится на жестком диске пользователя. Это окно оснащено кнопками для обращения к основным функциям системы.

Чтобы использовать электронные деньги для совершения покупок, пользователю нужны электронные монетки, хранящиеся на жестком диске. Перечисление денежного счета в банке на Ваш жесткий диск во многом напоминает работу банкомата. После щелчка на соответствующей кнопке панели инструментов появляется диалоговое окно. В этом окне пользователь указывает количество снимаемых со счета или помещаемых на счет денег.

Деньги могут быть потрачены двумя способами. Оплата может быть потребована кем-то, либо пользователь может инициировать оплату сам. В первом случае пользователь просто объявляет о своем согласии или несогласии платить. Чтобы инициировать оплату, пользователь щелкает мышью на значке оплаты и заполняет формы в диалоговом окне, которые используются для востребования оплаты. На них размещаются поля для ввода, идентификатора счета, денежной суммы, описание и пр.

У получателя денег есть выбор: перевести электронные деньги на свой банковский счет или записать их на свой жесткий диск в виде «монеток». Получатель указывает, что он желает получить оплату, а также в каком виде он хочет ее получить.

Пользователь системы с помощью панели инструментов может вызвать диалоговое окно, отображающее различные параметры счета пользователя, включая оплаченные заказы и полученные платежи.

Чтобы все это работало, а также обеспечивалась безопасность и конфиденциальность обеих сторон, необходимо применение сложных криптографических методов, некоторые из которых были изобретены и запатентованы Дэвидом Чаумом, основателем компании Digit Cash.

В заключение следует отметить, что для электронной коммерции было предложено множество электронных платежных систем. Нет никакого сомнения в том, что большая часть этих предложений окажется несостоятельными, и от них придется отказаться. Останется, вероятнее всего, несколько систем, так как у разных приложений могу быть различные требования.

11.8. Правовое обеспечение информационной безопасности

К правовым мерам обеспечения информационной безопасности относится: разработка норм, устанавливающих ответственность за компьютерные преступления; защита авторских прав программистов; совершенствование уголовного и гражданского законодательства, а также судопроизводства. К правовым мерам следует отнести также общественный контроль за разработчиками компьютерных систем и принятие соответствующих международных соглашений. До недавнего времени в Российской Федерации отсутствовала возможность эффективной борьбы с компьютерными преступлениями, так как данные преступления не могли считаться противозаконными, поскольку они не квалифицировались уголовным законодательством. До 1 января 1997 г. на уровне действующего законодательства России можно было считать удовлетворительно урегулированной лишь охрану авторских прав разработчиков программного обеспечения и, частично, защиту информации в рамках государственной тайны, но не были отражены права граждан на доступ к информации и защита информации, непосредственно связанные с компьютерными преступлениями.

Частично указанные проблемы были решены после введения в действие с 1 января 1997 г. нового Уголовного кодекса (УК), принятого Государственной Думой 24 мая 1996 г. В новом УК ответственность за компьютерные преступления устанавливают ст. ст. 272, 273 и 274. Ст. 272 нового УК устанавливает ответственность за неправомерный доступ к компьютерной информации (на машинном носителе в компьютере или сети компьютеров), если это привело либо к

уничтожению, блокированию, модификации или копированию информации, либо к нарушению работы вычислительной системы. (Под блокированием понимается такое воздействие на компьютер или компьютерную систему, которое повлекло временную или постоянную невозможность выполнять какие-либо операции над информацией.) Эта статья защищает право владельца на неприкосновенность информации в системе. Владельцем информационной системы может быть любое лицо, правомерно пользующееся услугами по обработке информации как собственник вычислительной системы или как лицо, которое приобрело право ее использования. Преступное деяние, ответственность за которое предусмотрено ст. 272, состоит в неправомерном доступе к охраняемой законом компьютерной информации, который всегда имеет характер совершения определенных действий и может выражаться в проникновении в компьютерную систему путем использования специальных технических или программных средств, позволяющих преодолеть установленные системой защиты; незаконного применения действующих паролей или маскировки под законного пользователя для проникновения в компьютер, хищения носителей информации (при условии, что были приняты меры их охраны), если это повлекло к уничтожению или блокированию информации. (Доступ считается правомерным, если он разрешен правообладателем, собственником информации или системы. Неправомерным является доступ, если лицо не имеет права доступа, либо имеет право на доступ, но осуществляет его с нарушением установленного порядка.) Для наступления уголовной ответственности обязательно должна существовать причинная связь между несанкционированным доступом к информации и наступлением предусмотренных ст. 272 последствий, тогда как случайное временное совпадение неправомерного доступа и сбоя в вычислительной системе, повлекшего указанные последствия, не влечет уголовной ответственности.

Неправомерный доступ к компьютерной информации должен осуществляться умышленно, т.е. совершая это преступление, лицо сознает, что неправомерно вторгается в компьютерную систему, предвидит возможность или неизбежность указанных в законе последствий, желает и сознательно допускает их наступление или относится к ним безразлично. Следовательно, с субъективной стороны преступление по ст. 272 характеризуется наличием прямого или кос-

венного умысла. Мотивы и цели данного преступления могут быть самыми разными: корыстными, направленными на причинение вреда (из хулиганских, конкурентных или иных побуждений) или проверку своих профессиональных способностей, и др. Поскольку мотив и цель преступления в ст. 272 не учитываются, она может применяться к всевозможным компьютерным посягательствам.

Ст. 272 УК состоит из двух частей. В первой части наиболее серьезное наказание преступника состоит в лишении свободы сроком до двух лет. Часть вторая указывает в качестве признаков, усиливающих уголовную ответственность, совершение преступления группой лиц или с использованием преступником своего служебного положения, а равно имеющим доступ к информационной системе, и допускает вынесение приговора сроком до пяти лет. При этом не имеет значения местонахождение объекта преступления (например, банка, к информации которого осуществлен неправомерный доступ в преступных целях), который может быть и зарубежным. По уголовному законодательству субъектами компьютерных преступлений могут быть лишь лица, достигшие 16-летнего возраста.

Ст. 272 УК не регулирует ситуации, когда неправомерный доступ к информации происходит по неосторожности, поскольку при расследовании обстоятельств доступа зачастую крайне трудно доказать преступный умысел. Так, при переходах по ссылкам от одного компьютера к другому в сети Интернет, связывающей миллионы компьютеров, можно легко попасть в защищаемую информационную зону какого-либо компьютера, даже не замечая этого (хотя целью могут быть и преступные посягательства).

Ст. 273 УК предусматривает уголовную ответственность за создание, использование и распространение вредоносных программ для компьютеров или модификацию программного обеспечения, заведомо приводящее к несанкционированному уничтожению, блокированию, модификации, копированию информации или к нарушению работы информационных систем. Статья защищает права владельца компьютерной системы на неприкосновенность хранящейся в ней информации. Вредоносными считаются любые программы, специально разработанные для нарушения нормального функционирования других компьютерных программ. Под нормальным функционированием понимается выполнение операций, для которых эти программы предназначены и которые определены

в документации на программу. Наиболее распространенные вредоносные программы – компьютерные вирусы, логические бомбы, а также программы, известные как «троянский конь». Для привлечения к ответственности по ст. 273 необязательно наступление каких-либо нежелательных последствий для владельца информации, достаточен сам факт создания вредоносных программ или внесение изменений в уже существующие программы, заведомо приводящих к указанным в статье последствиям. Использованием программ считается их выпуск в свет, воспроизведение, распространение и другие действия по введению в оборот. Использование программ может осуществляться путем записи в память компьютера или на материальный носитель, распространения по сетям или путем иной передачи другим пользователям.

Уголовная ответственность по ст. 273 возникает уже в результате создания вредоносных программ, независимо от их фактического использования. Даже наличие исходных текстов программ является основанием для привлечения к ответственности. Исключение составляет деятельность организаций, разрабатывающих средства противодействия вредоносным программам и имеющих соответствующие лицензии. Статья состоит из двух частей, различающихся признаком отношения преступника к совершаемым действиям. Ч. 1 предусматривает преступления, совершенные умышленно, с сознанием того, что создание, использование или распространение вредоносных программ заведомо должно привести к нарушению неприкосновенности информации. При этом ответственность наступает независимо от целей и мотивов посягательства, которые могут быть вполне позитивными (например, охрана личных прав граждан, борьба с техногенными опасностями, защита окружающей среды и т.п.). Максимальное наказание по первой части – лишение свободы сроком до трех лет. По ч. 2 дополнительный квалифицирующий признак – наступление тяжких последствий по неосторожности. В этом случае лицо сознает, что создает, использует или распространяет вредоносную программу или ее носители и предвидит возможность наступления серьезных последствий, но без достаточных оснований рассчитывает их предотвратить, или не предвидит этих последствий, хотя как высококвалифицированный программист мог и был обязан их предусмотреть. Поскольку последствия могут быть очень тяжкими (смерть или вред здоровью человека, опасность военной или

иной катастрофы, транспортные происшествия), максимальное наказание по ч. 2 – семь лет лишения свободы.

Отметим, что в законе не говорится о степени нанесенного вреда в отличие от краж, когда различаются просто кража, кража в крупном размере и кража в особо крупном размере. Здесь устанавливается лишь факт преступления, а размер ущерба влияет лишь на оценку его тяжести и меру ответственности.

Наконец, ст. 274 УК устанавливает ответственность за нарушение правил эксплуатации компьютеров, компьютерных систем или сетей лицом, имеющим доступ к ним, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации, если это деяние причинило существенный вред. Эта статья защищает интересы владельца компьютерной системы в отношении ее правильной эксплуатации и распространяется только на локальные вычислительные сети организаций. К глобальным вычислительным сетям, например к таким, как Интернет, эта статья неприменима. Под охраняемой законом информацией понимается информация, для которой в специальных законах установлен режим ее правовой защиты. Между фактом нарушения правил эксплуатации и наступившим существенным вредом должна быть обязательно установлена причинная связь и полностью доказано, что наступившие вредные последствия являются результатом именно нарушения правил. Оценку нанесенного вреда устанавливает суд, исходя из обстоятельств дела, причем считается, что существенный вред менее значителен, чем тяжкие последствия.

Субъект этой статьи – лицо, в силу своих должностных обязанностей имеющее доступ к компьютерной системе и обязанное соблюдать установленные для них технические правила. Согласно ч. 1 статьи он должен совершать свои деяния умышленно; сознавать, что нарушает правила эксплуатации; предвидеть возможность или неизбежность неправомерного воздействия на информацию и причинение существенного вреда, желать или сознательно допускать причинение такого вреда или относиться к его наступлению безразлично. Наиболее строгое наказание в этом случае – лишение права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет, или ограничение свободы на срок до двух лет. Ч. 2 ст. 274 предусматривает ответственность за те же деяния, не имевшие умысла, но повлекшие по неос-

торожности тяжкие последствия, например за установку инфицированной программы без антивирусной проверки, что повлекло за собой серьезные последствия (крупный финансовый ущерб, транспортные происшествия, утрата важных архивов, нарушение работы системы жизнеобеспечения в больнице и др.). Мера наказания за это преступление устанавливается судом в зависимости от наступивших последствий, максимальное наказание – лишение свободы на срок до четырех лет.

Как видно, рассмотренные статьи УК не охватывают все виды компьютерных преступлений, разнообразие которых увеличивается вместе с прогрессом в области компьютерной техники и ее использованием. Кроме того, некоторые формулировки статей допускают неоднозначное истолкование, например в определении злостного умысла. Поэтому в дальнейшем возможно пополнение и усовершенствование этих статей.

КОНТРОЛЬНЫЕ ВОПРОСЫ

1. В чем причины, связанные с необходимостью разработки новых методов защиты информации и дальнейшему развитию традиционных? На каких направлениях использования информационных систем эти методы особенно актуальны?

2. Какие непреднамеренные воздействия могут привести к потере информации, и каким образом осуществляется резервное копирование? Расскажите о защите от помех в электросетях. Что такое избыточность данных как метода защиты информации от непреднамеренных воздействий?

3. Определите, что означают следующие требования к методам защиты информации: целостность данных; доступность данных; секретность и конфедициальность; авторизация; аутентификация; запрещение повторного использования?

4. Какие методы защиты от локальных атак знаете?

5. Что такое криптография? Опишите традиционную схему шифрования открытым ключом. Назовите основные методы атаки на традиционную схему.

6. Расскажите, что такое электронная подпись. Назовите основные причины необходимости в ее специальной защите. Перечислите основные методы, применяемые для этих целей. Расскажите о защитной функции хэширования.