**ОСНОВЫ ЗАЩИТЫ ИНФОРМАЦИИ**

**Информационная безопасность (ИБ) и ее составляющие**

В вычислительной технике понятие безопасности является весьма широким. Оно подразумевает и надежность работы компьютера, и сохранность ценных данных, и защиту информации от внесения в нее изменений неуполномоченными лицами, и сохранение тайны переписки в электронной связи. Разумеется, во всех цивилизованных странах на страже безопасности граждан стоят законы, но в сфере вычислительной техники правоприменительная практика пока развита недостаточно, а законотворческий процесс не успевает за развитием технологий, поэтому надежность работы компьютерных систем во многом опирается на меры самозащиты.

Защита информации является актуальной, быстроразвивающейся, большой и сложной отраслью современных компьютерных технологий. Эта отрасль является многоплановой и многоуровневой. Она охватывает как порядок организации работы на отдельном компьютере, так и передачу разнообразных цифровых данных в локальных и глобальных компьютерных и телекоммуникационных сетях. Защита информации обеспечивается как на организационном, так и на техническом уровнях. К числу последних относятся как физические аппаратные, так и математические программные средства защиты информации, которые строятся на основе достижений новой науки – криптографии. К области защиты информации также относятся соответствующие разделы законодательства с комплексом юридических нормативных документов.

**Защита информации в компьютерных сетях**

При работе в Интернете следует иметь в виду, что насколько ресурсы Всемирной сети открыты каждому клиенту, настолько же и ресурсы его компьютерной системы могут быть при определенных условиях открыты всем, кто обладает необходимыми средствами.

Для частного пользователя этот факт не играет особой роли, но знать о нем необходимо, чтобы не допускать действий, нарушающих законодательства тех стран, на территории которых расположены серверы Интернета. К таким действиям относятся вольные или невольные попытки нарушить работоспособность компьютерных систем, попытки взлома защищенных систем, использование и распространение программ, нарушающих работоспособность компьютерных систем (в частности, компьютерных вирусов).

Работая во Всемирной сети, следует помнить о том, что абсолютно все действия фиксируются и протоколируются специальными программными средствами и информация как о законных, так и о незаконных действиях обязательно где-то накапливается. Таким образом, к обмену информацией в Интернете следует подходить как к обычной переписке с использованием почтовых открыток. Информация свободно циркулирует в обе стороны, но в общем случае она доступна всем участникам информационного процесса. Это касается всех служб Интернета, открытых для массового использования.

Однако даже в обычной почтовой связи наряду с открытками существуют и почтовые конверты. Использование почтовых конвертов при переписке не означает, что партнерам есть, что скрывать. Их применение соответствует давно сложившейся исторической традиции и устоявшимся морально-этическим нормам общения. Потребность в аналогичных “конвертах” для защиты информации существует и в Интернете. Сегодня Интернет является не только средством общения и универсальной справочной системой – в нем циркулируют договорные и финансовые обязательства, необходимость защиты которых как от просмотра, так и от фальсификации, очевидна. Начиная с 1999 года Интернет становится мощным средством обеспечения розничного торгового оборота, а это требует защиты данных кредитных карт и других электронных платежных средств.

Принципы защиты информации в Интернете опираются на определение информации, сформулированное нами в первой главе этого пособия. *Информация – это продукт взаимодействия данных и адекватных им методов.* Если в ходе коммуникационного процесса данные передаются через открытые системы (а Интернет относится именно к таковым), то исключить доступ к ним посторонних лиц невозможно даже теоретически. Соответственно, системы защиты сосредоточены на втором компоненте информации – на методах. Их принцип действия основан на том, чтобы исключить или, по крайней мере, затруднить возможность подбора *адекватного* метода для преобразования данных в информацию. Одним из приемов такой защиты является *шифрование* данных.

**Угрозы безопасности информации и их классификация**

Автоматизированные системы, обрабатывающие информацию, являются сложными техническими системами. Недостаточная надежность функционирования таких систем, сбои и отказы в работе тех или иных функциональных устройств, могут привести к потере информации.

В ряде случаев стоимость обрабатываемой информации значительно превосходит стоимость оборудования, входящего в состав автоматизированной системы. В таких ситуациях ставится задача сохранения информации даже в условиях производственных катастроф и стихийных бедствий.

Для того чтобы сформулировать задачи защиты информации от злоумышленников, необходимо представить себе их цели и возможности по достижению этих целей.

Обычно различают следующие цели нарушителя:

* незаконное завладение конфиденциальной информацией;
* модификация информации;
* уничтожение информации;
* нарушение функционирования АС;
* незаконное копирование программ (и другой ценной информации);
* отказ от информации

Под *конфиденциальной информацией* понимается информация, доступ к которой ограничен в соответствии с законодательством. Факт попадания такой информации злоумышленнику называют *утечкой информации* и говорят о *защите информации от утечки.* Утечка информации может быть разной по последствиям. Так, например, утечка информации, связанная с хищением носителя или даже компьютера в целом, очень быстро обнаруживается. В то же время негласная для законного владельца утечка информации наносит больший вред.

*Модификация информации* всегда подразумевается неявной для законного владельца информации. Модификация информации может проявляться по-разному. Например, в финансовом документе она может заключаться в "исправлении" номера счета, куда надо переслать деньги, или размера суммы, подлежащей перечислению по указанному адресу. В сетях с коммутацией пакетов модификация может заключаться в изъятии из канала связи части сообщения, изменение порядка следования частей сообщения. Наконец,

возможен повтор или посылка фальсифицированного сообщения, например, с указанием банку перечислить деньги.

*Уничтожение информации* может привести к краху вычислительной системы, если не были приняты профилактические меры по резервному копированию информации, и к временному выходу системы из строя при наличии резервных копий.

Под *нарушением функционирования* автоматизированной системы подразумевают (в отличие от уничтожения информации) скрытные действия, мешающие нормально функционировать системе. Такие действия могут осуществляться захватом ресурсов, запуска на решение посторонних задач или повышением приоритетности задач, не требующих срочного решения. К указанным вмешательствам в работу наиболее чувствительны информационные системы, работающие в режиме реального времени или в режиме оперативного принятия решений.

Говоря о *незаконном копировании программ*, имеют в виду копирование не конфиденциальной информации, а информации, распространяемой па коммерческой или другой договорной основе. Незаконное копирование программ и другой ценной информации рассматривается как нарушение авторских прав разработчиков программного продукта и баз данных.

*Отказ от информации* характерен для следующих ситуаций взаимодействия двух удаленных абонентов в телекоммуникационной сети. Если абонент А посылает абоненту В сообщение, а позднее отказывается от факта отправки такого сообщения, то говорят об *отказе от факта передачи сообщения*. Если абонент В получив сообщение от абонента А, позднее отказывается от факта получения сообщения, то говорят об отказе *от факта получения сообщения*. Первый случай реален, например, если посланное сообщение содержало некоторые обязательства отправителя по отношению к получателю, а второе – если полученное сообщение содержало некоторые поручения для получателя. Отказ от информации делает практически невозможным взаимодействие удаленных абонентов с использованием прогрессивных компьютерных и сетевых технологий.

При рассмотрении целей злоумышленника необходимо отметить следующее обстоятельство. При создании той или иной системы защиты информации в автоматизированной системе или сети, злоумышленник лишается возможности достичь своих целей наиболее простыми и доступными (как в отсутствие защиты) средствами. В новых условиях злоумышленник постарается исследовать внедренную систему защиты и найти пути ее преодоления. При этом у него появляются новые цели: узнать ключи или пароли, модифицировать программное обеспечение системы защиты информации и тем самым полностью или частично нейтрализовать защитный механизм, обойти его. Такие цели носят по сравнению со сформулированными выше промежуточный характер. Но эти цели надо обязательно учитывать при проектировании и внедрении средств защиты информации.

**Основные виды защиты информации**

В практической деятельности выделяют следующие основные виды защиты информации:

– защита информации от несанкционированного доступа:

– защита информации от перехвата в системах связи.

– защита юридической значимости электронных документов.

– защита конфиденциальной информации от утечки по каналам побочных электромагнитных излучении и наводок.

– защита информации от компьютерных вирусов и других опасных воздействии по каналам распространения программ.

– защита от несанкционированного копирования и распространения программ и ценной компьютерной информации.

Защита конфиденциальной и ценной информации от несанкционированного доступа (НСД) призвана обеспечить решение одной из двух наиболее важных задач защиты имущественных прав владельцев и пользователей ЭВМ – защиту собственности, воплощенной в обрабатываемой информации от всевозможных злоумышленных покушении, которые могут нанести существенный экономический и другой материальный и нематериальный ущерб К ней примыкает задача защиты государственных секретов, где в качестве собственника информации выступает государство Основной целью этого вида защиты является обеспечения конфиденциальности, целостности и доступности информации В части технической реализации защита от НСД сводится к задаче разграничения функциональных полномочии и доступа к информации

Существуют два принципа формулирования правил разграничения доступа дискреционный и мандатный.

Первый из них базируется *на* матричных моделях.

Пусть имеется некоторое множество поименованных объектов доступа (файлы, каталоги, устройства, и тому подобное) и некоторое множество субъектов доступа (пользователи, их процессы). Правила разграничения доступа тогда записываются в виде матрицы, каждый из столбцов которой соответствует одному объекту доступа, а каждая строка соответствует одному субъекту доступа. На пересечении *i*-го столбца и *j*-ой строки записываются права доступа *j*-го субъекта доступа к *i*-му объекту доступа (читать, записывать, удалять, и тому подобное).

На практике системы разграничения доступа, базирующиеся на матричных моделях, реализуются обычно в виде специальных компонент универсальных ОС или СУБД, либо в виде самостоятельных программных изделий. Существенной особенностью матричных средств разграничения доступа для наиболее используемых универсальных ОС является принципиальная децентрализованность механизмов диспетчера доступа, что приводит к невозможности строгого выполнения требований верифицируемости, защищенности и полноты контроля указанных механизмов.

Мандатный принцип разграничения доступа основан на том, что все объекты доступа наделяются метками конфиденциальности (например по грифам секретности: '"особой важности", "совершенно секретно", "секретно", "несекретно"), а для каждого субъекта доступа определяется уровень допуска (например уровень секретности документов, с которыми субъекту разрешено работать). Тогда при общении пользователя с системой чтение разрешается только по отношению к информации соответствующего уровня конфиденциальности или ниже. А запись информации разрешается только для информации соответствующего уровня конфиденциальности или выше. Такие правила обеспечивают при прохождении информации не понижение уровня ее конфиденциальности.

Отметим, что в наиболее ответственных случаях используются оба принципа формулирования правил разграничения доступа.

Сама процедура доступа пользователя (в соответствии с правилами разграничения доступа) происходит в три этапа: идентификация, аутентификация и авторизация.

*Идентификация* заключается в предъявлении пользователем системе своего идентификатора (имени) и проверке наличия в памяти системы этого имени.

*Аутентификация* заключается в проверке принадлежности субъекту доступа предъявленного им идентификатора (проверка подлинности). Для реализации процедуры аутентификации используется идентификатор субъекта доступа, который является либо его секретом (пароль и тому подобное), либо является уникальным для субъекта и гарантировано неподделываемым (биометрические характеристики).

Авторизация заключается в установлении прав доступа к тому или иному ресурсу в соответствии с правилами разграничения доступа.

Простейший способ защиты автоматизированной системы от удаленного доступа несанкционированных пользователей – это отказ от работы в сети, обеспечение физической защиты от всех внешних сетевых соединений. В наиболее ответственных случаях так и поступают.

Однако в силу практической невозможности такой изоляции в большинстве случаев в настоящее время, необходимо предусмотреть простые и ясные правила осуществления коммуникаций между локальными сетями различной степени защищенности, или даже, защищенной сети с незащищенной. Защищенная локальная сеть при этом представляется как бы находящейся внутри периметра, поддерживающего секретность. Внутри периметра служба контроля доступа и другие защитные механизмы определяют: кто и к какой информации допущен. В такой среде шлюзовая система, которая иногда называется брандмауэром, маршрутизатором или модулем защищенного интерфейса, может отделять защищенные системы или сети от незащищенных систем или сетей извне. Незащищенная система может общаться с защищенной только через единственный канал связи, контролируемый защищенным шлюзом. Шлюз контролирует трафик как извне, так и наружу, и эффективно изолирует защищенную сеть от внешнего мира. Благодаря тому, что брандмауэр защищает другие компьютеры, находящиеся внутри периметра, защита может быть сконцентрирована в брандмауэре.

**Методы защиты информации**

**Понятие о несимметричном шифровании информации**

Системам шифрования столько же лет, сколько письменному обмену информацией. Обычный подход состоит в том, что к документу применяется некий метод шифрования (назовем его *ключом),* после чего документ становится недоступен для чтения обычными средствами. Его можно прочитать только тот, кто знает ключ, только он может применить адекватный метод чтения. Аналогично происходит шифрование и ответного сообщения. Если в процессе обмена информацией для шифрования и чтения пользуются одним и тем же ключом, то такой криптографический процесс является *симметричным.*

Основной недостаток симметричного процесса заключается в том, что, прежде чем начать обмен информацией, надо выполнить передачу ключа, а для этого опять-таки нужна защищенная связь, то есть проблема повторяется, хотя и на другом уровне. Если рассмотреть оплату клиентом товара или услуги с помощью кредитной карты, то получается, что торговая фирма должна создать по одному ключу для каждого своего клиента и каким-то образом передать им эти ключи. Это крайне неудобно.

Поэтому в настоящее время в Интернете используют *несимметричные* криптографические системы, основанные на использовании не одного, а двух ключей. Происходит это следующим образом. Компания для работы с клиентами создает два ключа: один – *открытый* (*public – публичный*) ключ, а другой – *закрытый* (*private – личный*) ключ. На самом деле это как бы две “половинки” одного целого ключа, связанные друг с другом.

Ключи устроены так, что сообщение, зашифрованное одной половинкой, можно расшифровать только другой половинкой (не той, которой оно было закодировано). Создав пару ключей, торговая компания широко распространяет *публичный ключ* (открытую половинку) и надежно сохраняет *закрытый ключ* (свою половинку).

Как публичный, так и закрытый ключ представляют собой некую кодовую последовательность. Публичный ключ компании может быть опубликован на ее сервере, откуда каждый желающий может его получить. Если клиент хочет сделать фирме заказ, он возьмет ее публичный ключ и с его помощью закодирует свое сообщение о заказе и данные о своей кредитной карте. После кодирования это сообщение может прочесть только владелец закрытого ключа. Никто из участников цепочки, по которой пересылается информация, не в состоянии это сделать. Даже сам отправитель не может прочитать собственное сообщение, хотя ему хорошо известно содержание. Лишь получатель сможет прочесть сообщение, поскольку только у него есть закрытый ключ, дополняющий использованный публичный ключ.

Если фирме надо будет отправить клиенту квитанцию о том, что заказ принят к исполнению, она закодирует ее своим закрытым ключом. Клиент сможет прочитать квитанцию, воспользовавшись имеющимся у него публичным ключом данной фирмы. Он может быть уверен, что квитанцию ему отправила именно эта фирма, и никто иной, поскольку никто иной доступа к закрытому ключу фирмы не имеет.

**Принцип достаточности защиты**

Защита публичным ключом не является абсолютно надежной. Дело в том, что поскольку каждый желающий может получить и использовать чей-то публичный ключ, то он может сколь угодно подробно изучить алгоритм работы механизма шифрования и пытаться установить метод расшифровки сообщения, то есть *реконструировать закрытый ключ.*

Это настолько справедливо, что алгоритмы кодирования публичным ключом даже нет смысла скрывать. Обычно к ним есть доступ, а часто они просто широко публикуются. Тонкость заключается в том, что знание алгоритма еще не означает возможности провести реконструкцию ключа в *разумно приемлемые сроки.* Так, например, правила игры в шахматы известны всем, и нетрудно создать алгоритм для перебора всех возможных шахматных партий, но он никому не нужен, поскольку даже самый быстрый современный суперкомпьютер будет работать над этой задачей дольше, чем существует жизнь на нашей планете.

Количество комбинаций, которое надо проверить при реконструкции закрытого ключа, не столь велико, как количество возможных шахматных партий, однако защиту информации принято считать достаточной, если затраты на ее преодоление превышают ожидаемую ценность самой информации. В этом состоит *принцип достаточности защиты,* которым руководствуются при использовании несимметричных средств шифрования данных. Он предполагает, что защита не абсолютна, и приемы ее снятия известны, но она все же достаточна для того, чтобы сделать это мероприятие нецелесообразным. При появлении иных средств, позволяющих получить зашифрованную информацию в разумные сроки, изменяют принцип работы алгоритма, и проблема повторяется на более высоком уровне.

Разумеется, не всегда реконструкцию закрытого ключа производят методами простого перебора комбинаций. Для этого существуют специальные методы, основанные на исследовании особенностей взаимодействия открытого ключами с определенными структурами данных. Область науки, посвященная этим исследованиям, называется *криптоанализом,* а средняя продолжительность времени, необходимого для реконструкции закрытого ключа по его опубликованному открытому ключу, называется *криптостойкостъю* алгоритма шифрования.

Для многих методов несимметричного шифрования криптостойкость, полученная в результате криптоанализа, существенно отличается от величин, заявляемых разработчиками алгоритмов на основании теоретических оценок. Поэтому во многих странах вопрос применения алгоритмов шифрования данных находится в поле законодательного регулирования. В частности, в России к использованию в государственных и коммерческих организациях разрешены только те программные средства шифрования данных, которые прошли государственную сертификацию в административных органах, в частности, в Федеральном агентстве правительственной связи и информации при Президенте Российской Федерации (ФАПСИ).

**Понятие об электронной подписи**

Методы несимметричного шифрования легли также в основу идеи *электронной цифровой подписи*. В самом упрощенном виде идея цифровой подписи заключается в следующем.

Отправитель документа шифрует свое сообщение определенным образом с помощью своего уникального закрытого ключа. Затем он посылает сам документ и его шифровку адресату вместе с открытым ключом. Адресат, получив шифровку и документ, расшифровывает шифровку. В случае полного совпадения расшифрованного документа и открытого документа он может быть уверен, что документ пришел именно от отправителя, а не от другого постороннего лица, или что документ не был изменен злоумышленником или искажен в процессе пересылки. Так обеспечивается аутентификация, т.е. удостоверение подлинности документа. По сути, это визирование документа электронным способом.

На практике системы электронной подписи используют шифрование не самого документа, который может быть достаточно объемным (или документ должен оставаться открытым для просмотра всеми желающими лицами), а только его «выжимки». Для получения такой короткой «выжимки» используют так называемую процедуру «хэширования». Хэширование (hash function – буквально, получение «смеси») по своей природе принадлежит классу необратимых математических преобразований. В результате хеширования документа получается короткий код, состоящий всего из 128 бит. Этот короткий и уникальный для данного документа хэш-код и является цифровой подписью. Любое изменение исходного документа приведет к изменению его хэш-кода, и наоборот, нет двух различных документов, имеющих одинаковый хэш-код (128-битный код, несмотря на свою компактность – это очень большое двоичное число; количество всевозможных комбинаций данного кода превышает полный возраст всей нашей Вселенной, даже если исчислять его в секундах).

После получения хэш-кода его шифруют закрытым ключом и вместе с исходным документом посылают по открытым каналам связи нужным адресатам. Абонент-получатель, получив документ вместе с шифрованным хэш-кодом, производит следующие действия. Вначале с помощью той же процедуры хэширования (которая не является секретной), примененной к принятому документу, получается новая копия хэш-кода. Затем с помощью открытого ключа расшифровывается принятый оригинальный хэш-код. В случае подлинности документа два хэш-кода (вновь полученный и принятый) должны совпасть. При искажении документа даже на один символ хэш-коды не совпадут.

Таким образом, в системах электронной подписи методами шифрования защищается не содержание документа, а удостоверение его подлинности. В случае, когда само содержание документа должно оставаться скрытым, процедуру шифрования просто применяют и к самому документу тоже.

**Понятие об электронных сертификатах**

Системой несимметричного шифрования обеспечивается делопроизводство в Интернете. Благодаря ей каждый из участников обмена может быть уверен, что полученное сообщение отправлено именно тем, кем оно подписано. Однако здесь возникает еще ряд проблем, например проблема регистрации даты отправки сообщения. Такая проблема возникает во всех случаях, когда через Интернет заключаются договоры между сторонами. Отправитель документа может легко изменить текущую дату средствами настройки операционной системы. Поэтому обычно дата и время отправки электронного документа не имеют юридической силы. В тех же случаях, когда это важно, выполняют сертификацию даты/времени.

**Сертификация даты**

Сертификация даты выполняется при участии третьей, независимой стороны. Например, это может быть сервер организации, авторитет которой в данном вопросе признают оба партнера. В этом случае документ, зашифрованный открытым ключом партнера и снабженный своей электронной подписью, отправляется сначала на сервер сертифицирующей организации. Там он получает “приписку” с указанием точной даты и времени, зашифрованную закрытым ключом этой организации. Партнер декодирует содержание документа, электронную подпись отправителя и отметку о дате с помощью своих “половинок” ключей. Вся работа автоматизирована.

**Сертификация Web-узлов**

Сертифицировать можно не только даты. При заказе товаров в Интернете важно убедиться в том, что сервер, принимающий заказы и платежи от имени некоей фирмы, действительно представляет эту фирму. Тот факт, что он распространяет ее открытый ключ и обладает ее закрытым ключом, строго говоря, еще ничего не доказывает, поскольку за время, прошедшее после создания ключа, он мог быть скомпрометирован. Подтвердить действительность ключа тоже может третья организация путем выдачи сертификата продавцу. В сертификате указано, когда он выдан и на какой срок. Если добросовестному продавцу станет известно, что его закрытый ключ каким-либо образом скомпрометирован, он сам уведомит сертификационный центр, старый сертификат будет аннулирован, создан новый ключ и выдан новый сертификат.

Прежде чем выполнять платежи через Интернет или отправлять данные о своей кредитной карте кому-либо, следует проверить наличие действующего сертификата у получателя путем обращения в сертификационный центр. Это называется *сертификацией Web-узлов*.

**Сертификация издателей**

Схожая проблема встречается и при распространении программного обеспечения через Интернет. Так, например, мы указали, что Web-браузеры, служащие для просмотра Web-страниц, должны обеспечивать механизм защиты от нежелательного воздействия активных компонентов на компьютер клиента. Можно представить, что произойдет, если кто-то от имени известной компании начнет распространять модифицированную версию ее браузера, в которой специально оставлены бреши в системе защиты. Злоумышленник может использовать их для активного взаимодействия с компьютером, на котором работает такой браузер.

Это относится не только к браузерам, но и ко всем видам программного обеспечения, получаемого через Интернет, в которое могут быть имплантированы “троянские кони”, “компьютерные вирусы”, “часовые бомбы” и прочие нежелательные объекты, в том числе и такие, которые невозможно обнаружить антивирусными средствами. Подтверждение того, что сервер, распространяющий программные продукты от имени известной фирмы, действительно уполномочен ею для этой деятельности, осуществляется путем *сертификации издателей.* Она организована аналогично сертификации Web-узлов.

Средства для проверки сертификатов обычно предоставляют броузеры. В частности, в обозревателе Microsoft Internet Explorer 5.0, работа с которым более подробно будет рассмотрена в следующей главе, доступ к центрам сертификации осуществляется командой Сервис > Свойства обозревателя *>* Содержание *>* Сертификатов > Доверенные корневые центры сертификации.

**Антивирусная защита**

**Виды компьютерных вирусов**

Компьютерный вирус – это программный код, встроенный в другую программу, или в документ, или в определенные области носителя данных и предназначенный для выполнения несанкционированных действий на несущем компьютере. Основными типами компьютерных вирусов являются:

* программные вирусы;
* загрузочные вирусы;
* макровирусы.

К компьютерным вирусам примыкают и так называемые *троянские кони (троянские программы, троянцы).*

Программные вирусы – это блоки программного кода, целенаправленно внедренные внутрь других прикладных программ. При запуске программы, несущей вирус, происходит запуск имплантированного в нее вирусного кода. Работа этого кода вызывает скрытые от пользователя изменения в файловой системе жестких дисков и/или в содержании других программ. Так, например, вирусный код может воспроизводить себя в теле других программ – этот процесс называется *размножением.* По прошествии определенного времени, создав достаточное количество копий, программный вирус может перейти к разрушительным действиям – нарушению работы программ и операционной системы, удалению информации, хранящейся на жестком диске. Этот процесс называется *вирусной атакой.*

Самые разрушительные вирусы могут инициировать форматирование жестких дисков. Поскольку форматирование диска – достаточно продолжительный процесс, который не должен пройти незамеченным со стороны пользователя, во многих случаях программные вирусы ограничиваются уничтожением данных только в системных секторах жесткого диска, что эквивалентно потере таблиц файловой структуры. В этом случае данные на жестком диске остаются нетронутыми, но воспользоваться ими без применения специальных средств нельзя, поскольку неизвестно, какие сектора диска каким файлам принадлежит. Теоретически восстановить данные в этом случае можно, но трудоемкость этих работ исключительно высока.

Считается, что никакой вирус не в состоянии вывести из строя аппаратное обеспечение компьютера. Однако бывают случаи, когда аппаратное и программное обеспечение настолько взаимосвязаны, что программные повреждения приходится устранять заменой аппаратных средств. Так, например, в большинстве современных материнских плат базовая система ввода-вывода (*BIOS*) хранится в перезаписываемых постоянных запоминающих устройствах (так называемая *флэш-память*). Возможность перезаписи информации в микросхеме флэш-памяти используют некоторые программные вирусы для уничтожения данных *BIOS.* В этом случае для восстановления работоспособности компьютера требуется либо замена микросхемы, хранящей *BIOS,* либо ее перепрограммирование на специальных устройствах, называемых *программаторами.*

Программные вирусы поступают на компьютер при запуске непроверенных программ, полученных на внешнем носителе (гибкий диск, компакт-диск и т. п.) или принятых из Интернета. Особое внимание следует обратить на слова *при запуске.* При обычном копировании зараженных файлов заражение компьютера произойти не может. В связи с этим все данные, принятые из Интернета, должны проходить обязательную проверку на безопасность, а если получены незатребованные данные из незнакомого источника, их следует уничтожать, не рассматривая. Обычный прием распространения “троянских” программ – приложение к электронному письму с “рекомендацией” извлечь и запустить якобы полезную программу.

От программных вирусов загрузочные вирусы отличаются методом распространения. Они поражают не программные файлы, а определенные системные области магнитных носителей (гибких и жестких дисков). Кроме того, на включенном компьютере они могут временно располагаться в оперативной памяти.

Обычно заражение происходит при попытке загрузки компьютера с магнитного носителя, системная область которого содержит загрузочный вирус. Так, например, при попытке загрузить компьютер с гибкого диска происходит сначала проникновение вируса в оперативную память, а затем в загрузочный сектор жестких дисков. Далее этот компьютер сам становится источником распространения загрузочного вируса.

Макровирусы – это особая разновидность вирусов поражает документы, выполненные в некоторых прикладных программах, имеющих средства для исполнения так называемых *макрокоманд.* В частности, к таким документам относятся документы текстового процессора Microsoft Word (они имеют расширение .DOC). Заражение происходит при открытии файла документа в окне программы, если в ней не отключена возможность исполнения макрокоманд. Как и для других типов вирусов, результат атаки может быть как относительно безобидным, так и разрушительным.

**Методы и средства защиты от компьютерных вирусов**

Существуют три рубежа защиты от компьютерных вирусов:

* предотвращение поступления вирусов;
* предотвращение вирусной атаки, если вирус все-таки поступил на компьютер;
* предотвращение разрушительных последствий, если атака все-таки произошла. Существуют три метода реализации защиты:
* программные методы защиты;
* аппаратные методы защиты;
* организационные методы защиты.

В вопросе защиты ценных данных часто используют бытовой подход: “болезнь лучше предотвратить, чем лечить”. К сожалению, именно он и вызывает наиболее разрушительные последствия. Создав бастионы на пути проникновения вирусов в компьютер, нельзя положиться на их прочность и остаться неготовым к действиям после разрушительной атаки. К тому же, вирусная атака – далеко не единственная и даже не самая распространенная причина утраты важных данных. Существуют программные сбои, которые могут вывести из строя операционную систему, а также аппаратные сбои, способные сделать жесткий диск неработоспособным. Всегда существует вероятность утраты компьютера вместе с ценными данными в результате кражи, пожара или иного стихийного бедствия.

Поэтому создавать систему безопасности следует в первую очередь “с конца” – с предотвращения разрушительных последствий любого воздействия, будь то вирусная атака, кража в помещении или физический выход жесткого диска из строя. Надежная и безопасная работа с данными достигается только тогда, когда любое неожиданное событие, в том числе и полное физическое уничтожение компьютера не приведет к катастрофическим последствиям.

Основным средством защиты информации является резервное копирование наиболее ценных данных. В случае утраты информации по любой из вышеперечисленных причин жесткие диски переформатируют и подготавливают к новой эксплуатации. На “чистый” отформатированный диск устанавливают операционную систему с дистрибутивного компакт-диска, затем под ее управлением устанавливают все необходимое программное обеспечение, которое тоже берут с дистрибутивных носителей. Восстановление компьютера завершается восстановлением данных, которые берут с резервных носителей.

При резервировании данных следует также иметь в виду и то, что надо отдельно сохранять все регистрационные и парольные данные для доступа к сетевым службам Интернета. Их не следует хранить на компьютере. Обычное место хранения – служебный дневник в сейфе руководителя подразделения.

Создавая план мероприятий по резервному копированию информации, необходимо учитывать, что резервные копии должны храниться отдельно от компьютера. То есть, например, резервирование информации на отдельном жестком диске того же компьютера только создает иллюзию безопасности. Относительно новым и достаточно надежным приемом хранения ценных, но неконфиденциальных данных является их хранение в Web-папках на удаленных серверах в Интернете. Есть службы, бесплатно предоставляющие пространство (до нескольких Мбайт) для хранения данных пользователя.

Резервные копии конфиденциальных данных сохраняют на внешних носителях, которые хранят в сейфах, желательно в отдельных помещениях. При разработке организационного плана резервного копирования учитывают необходимость создания не менее двух резервных копий, сохраняемых в разных местах. Между копиями *осуществляют ротацию.* Например в течение недели ежедневно копируют данные на носители резервного комплекта А, а через неделю их заменяют комплектом Б, и т. д.

Вспомогательными средствами защиты информации являются антивирусные программы и средства аппаратной защиты. Так, например, простое отключение перемычки на материнской плате не позволит осуществить стирание перепрограммируемой микросхемы ПЗУ (флэш-BIOS), независимо от того, кто будет пытаться это сделать: компьютерный вирус, злоумышленник или неаккуратный пользователь.

Существует достаточно много программных средств антивирусной защиты. Они предоставляют следующие возможности.

1. *Создание образа жесткого диска на внешних носителях* (например, на гибких дисках). В случае выхода из строя данных в системных областях жесткого диска сохраненный “образ диска” может позволить восстановить если не все данные, то по крайней мере их большую часть. Это же средство может защитить от утраты данных при аппаратных сбоях и при неаккуратном форматировании жесткого диска.
2. Регулярное сканирование жестких дисков в поисках компьютерных вирусов. Сканирование обычно выполняется автоматически при каждом включении компьютера и при размещении внешнего диска в считывающем устройстве. При сканировании следует иметь в виду, что антивирусная программа ищет вирус путем сравнения кода программ с кодами известных ей вирусов, хранящимися в базе данных. Если база данных устарела, а вирус является новым, сканирующая программа его не обнаружит. Для надежной работы следует регулярно обновлять антивирусную программу. Желательная периодичность обновления – один раз в две недели; допустимая – один раз в три месяца. Для примера укажем, что разрушительные последствия атаки вируса W95.CIH.1075 (“Чернобыль”), вызвавшего уничтожение информации на сотнях тысяч компьютеров 26 апреля 1999 года, были связаны не с отсутствием средств защиты от него, а с длительной задержкой (более года) в обновлении этих средств.
3. Контроль за изменением размеров и других атрибутов файлов. Поскольку некоторые компьютерные вирусы на этапе размножения изменяют параметры зараженных файлов, контролирующая программа может обнаружить их деятельность и предупредить пользователя.
4. Контроль за обращениями к жесткому диску. Поскольку наиболее опасные операции, связанные с работой компьютерных вирусов, так или иначе обращены на модификацию данных, записанных на жестком диске, антивирусные программы могут контролировать обращения к нему и предупреждать пользователя о подозрительной активности.