# Тема 10

# Основы защиты информации

## 10.1. Защита информации как закономерность развития компьютерных систем

*Защита информации* – это применение различных средств и методов, использование мер и осуществление мероприятий для того, чтобы обеспечить систему надежности передаваемой, хранимой и обрабатываемой информации.

Защита информации включает в себя:

• обеспечение физической целостности информации, исключение искажений или уничтожения элементов информации;

• недопущение подмены элементов информации при сохранении ее целостности;

• отказ в несанкционированном доступе к информации лицам или процессам, которые не имеют на это соответствующих полномочий;

• приобретение уверенности в том, что передаваемые владельцем информационные ресурсы будут применяться только в соответствии с обговоренными сторонами условиями.

Процессы по нарушению надежности информации подразделяют на случайные и злоумышленные (преднамеренные). Источниками *случайных* разрушительных процессов являются непреднамеренные, ошибочные действия людей, технические сбои. *Злоумышленные* нарушения появляются в результате умышленных действий людей.

Проблема защиты информации в системах электронной обработки данных возникла практически одновременно с их созданием. Ее вызвали конкретные факты злоумышленных действий над информацией.

Важность проблемы по предоставлению надежности информации подтверждается затратами на защитные мероприятия. Для обеспечения надежной системы защиты необходимы значительные материальные и

финансовые затраты. Перед построением системы защиты должна быть разработана оптимизационная модель, позволяющая достичь максимального результата при заданном или минимальном расходовании ресурсов. Расчет затрат, которые необходимы для предоставления требуемого уровня защищенности информации, следует начинать с выяснения нескольких фактов: полного перечня угроз информации, потенциальной опасности для информации каждой из угроз, размера затрат, необходимых для нейтрализации каждой из угроз.

Если в первые десятилетия активного использования ПК основную опасность представляли хакеры, подключившиеся к компьютерам в основном через телефонную сеть, то в последнее десятилетие нарушение надежности информации прогрессирует через программы, компьютерные вирусы, глобальную сеть Интернет.

Имеется достаточно много способов несанкционированного доступа к информации, в том числе:

• просмотр;

• копирование и подмена данных;

• ввод ложных программ и сообщений в результате подключения к каналам связи;

• чтение остатков информации на ее носителях;

• прием сигналов электромагнитного излучения и волнового характера;

• использование специальных программ.

Для борьбы со всеми этими способами несанкционированного доступа необходимо разрабатывать, создавать и внедрять многоступенчатую непрерывную и управляемую архитектуру безопасности информации. Защищать следует не только информацию конфиденциального содержания. На объект защиты обычно действует некоторая совокупность дестабилизирующих факторов. При этом вид и уровень воздействия одних факторов могут не зависеть от вида и уровня других.

Возможна ситуация, когда вид и уровень взаимодействия имеющихся факторов существенно зависят от влияния других, явно или скрыто усиливающих такие воздействия. В этом случае следует применять как независимые с точки зрения эффективности защиты средства, так и взаимозависимые. Для того чтобы обеспечить достаточно высокий уровень безопасности данных, надо найти компромисс между стоимостью защитных мероприятий, неудобствами при использовании мер защиты и важностью защищаемой информации. На основе детального анализа многочисленных взаимодействующих факторов можно найти разумное и эффективное решение о сбалансированности мер защиты от конкретных источников опасности.

## 10.2. Объекты и элементы защиты в компьютерных системах обработки данных

*Объект защиты* – это такой компонент системы, в котором находится защищаемая информация. *Элементом защиты* является совокупность данных, которая может содержать необходимые защите сведения.

При деятельности компьютерных систем могут возникать:

• отказы и сбои аппаратуры;

• системные и системотехнические ошибки;

• программные ошибки;

• ошибки человека при работе с компьютером.

Несанкционированный доступ к информации возможен во время технического обслуживания компьютеров в процессе прочтения информации на машинных и других носителях. Незаконное ознакомление с информацией разделяется на пассивное и активное. При *пассивном* ознакомлении с информацией не происходит нарушения информационных ресурсов и нарушитель может лишь раскрывать содержание сообщений. В случае *активного* несанкционированного ознакомления с информацией есть возможность выборочно изменить, уничтожить порядок сообщений, перенаправить сообщения, задержать и создать поддельные сообщения.

Для обеспечения безопасности проводятся разные мероприятия, которые объединены понятием «система защиты информации».

*Система защиты информации* – это совокупность организационных (административных) и технологических мер, программно-технических средств, правовых и морально-этических норм, которые применяются для предотвращения угрозы нарушителей с целью сведения до минимума возможного ущерба пользователям и владельцам системы.

*Организационно-административными средствами защиты* называется регламентация доступа к информационным и вычислительным ресурсам, а также функциональным процессам систем обработки данных. Эти средства защиты применяются для затруднения или исключения возможности реализации угроз безопасности. Наиболее типичными организационно-административными средствами являются:

• допуск к обработке и передаче охраняемой информации только проверенных должностных лиц;

• хранение носителей информации, которые представляют определенную тайну, а также регистрационных журналов в сейфах, недоступных для посторонних лиц;

• учет применения и уничтожения документов (носителей) с охраняемой информацией;

• разделение доступа к информационным и вычислительным ресурсам должностных лиц в соответствии с их функциональными обязанностями.

*Технические средства защиты* применяются для создания некоторой физически замкнутой среды вокруг объекта и элементов защиты. При этом используются такие мероприятия, как:

• ограничение электромагнитного излучения через экранирование помещений, в которых осуществляется обработка информации;

• реализация электропитания оборудования, отрабатывающего ценную информацию, от автономного источника питания или общей электросети через специальные сетевые фильтры.

*Программные средства и методы защиты* являются более активными, чем другие применяемые для защиты информации в ПК и компьютерных сетях. Они реализуют такие функции защиты, как разграничение и контроль доступа к ресурсам; регистрация и изучение протекающих процессов; предотвращение возможных разрушительных воздействий на ресурсы; криптографическая защита информации.

Под *технологическими средствами защиты информации* понимаются ряд мероприятий, органично встраиваемых в технологические процессы преобразования данных. В них также входят:

• создание архивных копий носителей;

• ручное или автоматическое сохранение обрабатываемых файлов во внешней памяти компьютера;

• автоматическая регистрация доступа пользователей к различным ресурсам;

• выработка специальных инструкций по выполнению всех технологических процедур и др.

*Правовые* и *морально-этические меры и средства защиты* включают в себя действующие в стране законы, нормативные акты, регламентирующие правила, нормы поведения, соблюдение которых способствует защите информации.

### 10.3. Средства опознания и разграничения доступа к информации

*Идентификацией* называется присвоение тому или иному объекту или субъекту уникального имени или образа. *Аутентификация* – это установление подлинности объекта или субъекта, т. е. проверка, является ли объект (субъект) тем, за кого он себя выдает.

Конечная цель процедур идентификации и аутентификации объекта (субъекта) заключается в допуске его к информации ограниченного пользования в случае положительной проверки либо отказе в допуске при отрицательном результате проверки.

Объекты идентификации и аутентификации включают в себя: людей (пользователей, операторов); технические средства (мониторы, рабочие станции, абонентские пункты); документы (ручные, распечатки); магнитные носители информации; информацию на экране монитора.

К наиболее распространенным методам аутентификации относятся присвоение лицу или другому имени пароля и хранение его значения в вычислительной системе. *Паролем* называется совокупность символов, которая определяет объект (субъект).

Пароль как средство обеспечения безопасности способен использоваться для идентификации и установления подлинности терминала, с которого входит в систему пользователь, а также для обратного установления подлинности компьютера по отношению к пользователю.

С учетом важности пароля как средства повышения безопас – ности информации от несанкционированного использования необходимо соблюдать следующие меры предосторожности:

1) не хранить пароли в вычислительной системе в незашифрованном месте;

2) не печатать и не отображать пароли в открытом виде на терминале пользователя;

3) не применять в качестве пароля свое имя или имена родственников, а также личную информацию (дата рождения, номер домашнего или служебного телефона, название улицы);

4) не применять реальные слова из энциклопедии или толкового словаря;

5) использовать длинные пароли;

6) применять смесь символов верхнего и нижнего регистров клавиатуры;

7) применять комбинации из двух простых слов, соединенных специальными символами (например, +,=,<);

8) использовать несуществующие новые слова (абсурдные или даже бредового содержания);

9) как можно чаще менять пароль.

Для идентификации пользователей могут использоваться сложные в плане технической реализации системы, которые обеспечивают установление подлинности пользователя на основе анализа его индивидуальных параметров: отпечатков пальцев, рисунка линий руки, радужной оболочки глаз, тембра голоса. Наиболее широкое применение имеют физические методы идентификации, которые используют носители кодов паролей. Такими носителями могут быть пропуск в контрольно-пропускных системах; пластиковые карты с именем владельца, его кодом, подписью; пластиковые карточки с магнитной полосой, которая считывается специальным считывающим устройством; пластиковые карты, содержащие встроенную микросхему; карты оптической памяти.

Одним из наиболее интенсивно разрабатываемых направлений по обеспечению безопасности информации является идентификация и определение подлинности документов на основе электронной цифровой подписи. При передаче информации по каналам связи используется факсимильная аппаратура, но при этом к получателю приходит не подлинник, а только копия документа с копией подписи, которая в процессе передачи может быть подвергнута повторному копированию для использования ложного документа.

*Электронная цифровая подпись* представляет собой способ шифрования с использованием криптографического преобразования и является паролем, зависящим от отправителя, получателя и содержания передаваемого сообщения. Для того чтобы предупредить повторное использование подписи, ее необходимо менять от сообщения к сообщению.

### 10.4. Криптографический метод защиты информации

Наиболее эффективным средством повышения безопасности является криптографическое преобразование. Для того чтобы повысить безопасность, осуществляется одно из следующих действий:

1) передача данных в компьютерных сетях;

2) передача данных, которые хранятся в удаленных устройствах памяти;

3) передача информации при обмене между удаленными объектами.

Защита информации методом криптографического преобразования состоит в приведении ее к неявному виду через преобразование составных частей информации (букв, цифр, слогов, слов) с применением специальных алгоритмов либо аппаратных средств и кодов ключей. *Ключ* является изменяемой частью криптографической системы, хранящейся в тайне и определяющей, какое шифрующее преобразование из возможных выполняется в данном случае.

Для изменения (шифрования) используется некоторый алгоритм или устройство, реализующее заданный алгоритм. Алгоритмы могут быть известны широкому кругу лиц. Управление процессом шифрования происходит с помощью периодически меняющегося кода ключа, который обеспечивает каждый раз оригинальное представление информации в случае применения одного и того же алгоритма или устройства. При известном ключе можно относительно быстро, просто и надежно расшифровать текст. Без знания ключа эта процедура может стать практически невыполнимой даже при использовании компьютера.

К методам криптографического преобразования предъявляются следующие необходимые требования:

1) он должен быть достаточно устойчивым к попыткам раскрытия исходного текста с помощью использования зашифрованного;

2) обмен ключа не должен быть тяжел для запоминания;

3) затраты на защитные преобразования следует сделать приемлемыми при заданном уровне сохранности информации;

4) ошибки в шифровании не должны вызывать явную потерю информации;

5) размеры зашифрованного текста не должны превышать размеры исходного текста.

Методы, предназначенные для защитных преобразований, подразделяют на четыре основные группы: перестановки, замены (подстановки), аддитивные и комбинированные методы.

Методы *перестановки и замены (подстановки)* характеризуются коротким ключей, а надежность защиты определяется сложностью алгоритмов преобразования. Для *аддитивных* методов, наоборот, свойственны простые алгоритмы и длинные ключи. *Комбинированные методы* являются более надежными. Они чаще всего сочетают в себе достоинства используемых компонентов.

Упомянутые четыре метода криптографического преобразования относятся к методам симметричного шифрования. Один ключ используется и для шифрования, и для дешифрования.

Основными методами криптографического преобразования являются методы перестановки и замены. Основа метода *перестановки* состоит в разбиении исходного текста на блоки, а затем в записи этих блоков и чтении шифрованного текста по разным путям геометрической фигуры.

Шифрование методом *замены* заключается в том, что символы исходного текста (блока), записанные в одном алфавите, заменяются символами другого алфавита в соответствии с используемым ключом преобразования.

Комбинация этих методов привела к образованию метода *производного шифра,* который обладает сильными криптографическими возможностями. Алгоритм метода реализуется как аппаратно, так и программно, но рассчитан на реализацию с помощью электронных устройств специального назначения, что позволяет достичь высокой производительности и упрощенной организации обработки информации. Налаженное в некоторых странах Запада

промышленное производство аппаратуры для криптографического шифрования позволяет резко увеличить уровень безопасности коммерческой информации при ее хранении и электронном обмене в компьютерных системах.

### 10.5. Компьютерные вирусы

*Компьютерный вирус* – это специально написанная программа, способная самопроизвольно присоединяться к другим программам (заражать их), создавать свои копии и внедрять их в файлы, системные области компьютера и другие объединенные с ним компьютеры в целях нарушения нормальной работы программ, порчи файлов и каталогов, а также создания разных помех при работе на компьютере.

Появление вирусов в компьютере определяется по следующим наблюдаемым признакам:

- уменьшение производительности работы компьютера;
- невозможность и замедление загрузки ОС;
- повышение числа файлов на диске;
- замена размеров файлов;
- периодическое появление на экране монитора неуместных сообщений;
- уменьшение объема свободной ОП;
- резкое возрастание времени доступа к жесткому диску;
- разрушение файловой структуры;
- загорание сигнальной лампочки дисковода, когда к нему нет обращения.

Основными путями заражения компьютеров вирусами обычно служат съемные диски (дискеты и CD-ROM) и компьютерные сети. Заражение жесткого диска компьютера может произойти в случае загрузки компьютера с дискеты, содержащей вирус.

По тому, какой вид среды обитания имеют вирусы, их классифицируют на загрузочные, файловые, системные, сетевые и файлово – загрузочные (многофункциональные).

*Загрузочные вирусы* внедряются в загрузочный сектор диска или в сектор, который содержит программу загрузки системного диска.

*Файловые вирусы* помещаются в основном в исполняемых файлах с расширением .COM и .EXE.

*Системные вирусы* внедряются в системные модули и драйверы периферийных устройств, таблицы размещения файлов и таблицы разделов.

*Сетевые вирусы* находятся в компьютерных сетях, а *файлово-загрузочные* – заражают загрузочные секторы дисков и файлы прикладных программ.

По пути заражения среды обитания вирусы разделяются на резидентные и нерезидентные.

*Резидентные вирусы* при заражении компьютера оставляют в ОП свою резидентную часть, которая после заражения перехватывает обращение ОС к другим объектам заражения, внедряется в них и выполняет свои разрушительные действия, которые могут привести к выключению или перезагрузке компьютера. *Нерезидентные вирусы* не заражают ОП компьютера и проявляют активность ограниченное время.

Особенность построения вирусов влияет на их проявление и функционирование.

*Логическая бомба* является программой, которая встраивается в большой программный комплекс. Она безвредна до наступления определенного события, после которого реализуется ее логический механизм.

*Программы-мутанты,* самовоспроизводясь, создают копии, явно отличающиеся от оригинала.

*Вирусы-невидимки,* или стелс-вирусы, перехватывают обращения ОС к пораженным файлам и секторам дисков и подставляют вместо себя незараженные объекты. Эти вирусы при обращении к файлам применяют достаточно оригинальные алгоритмы, позволяющие «обманывать» резидентные антивирусные мониторы.

*Макровирусы* используют возможности макроязыков, которые встроены в офисные программы обработки данных (текстовые редакторы, электронные таблицы).

По степени воздействия на ресурсы компьютерных систем и сетей, или по деструктивным возможностям, выделяют безвредные, неопасные, опасные и разрушительные вирусы.

*Безвредные вирусы* не оказывают патологического влияния на работу компьютера. *Неопасные вирусы* не разрушают файлы, однако уменьшают свободную дисковую память, выводят на экран графические эффекты. *Опасные вирусы* часто вызывают значительные нарушения в работе компьютера. *Разрушительные вирусы* могут привести к стиранию информации, полному или частичному нарушению работы прикладных программ. Важно иметь в виду, что любой файл, способный к загрузке и выполнению кода программы, является потенциальным местом, где может помещаться вирус.

### 10.6. Антивирусные программы

Широкое распространение компьютерных вирусов привело к разработке антивирусных программ, которые позволяют обнаруживать и уничтожать вирусы, «лечить» пораженные ресурсы.

Основой работы большинства антивирусных программ является принцип поиска сигнатуры вирусов. *Вирусной сигнатурой* называют некоторую уникальную характеристику вирусной программы, выдающую присутствие вируса в компьютерной системе. Чаще всего в антивирусные программы включается периодически обновляемая база данных сигнатур вирусов. Антивирусная программа изучает и анализирует компьютерную систему, а также проводит сравнение, отыскивая соответствие с сигнатурами в базе данных. Если программа находит соответствие, она старается вычистить обнаруженный вирус.

По способу работы антивирусные программы можно разделить на фильтры, ревизоры, доктора, детекторы, вакцины и др.

*Программы-фильтры* – это «сторожа», которые постоянно находятся в ОП. Они являются резидентными и перехватывают все запросы к ОС на выполнение подозрительных действий, т. е. операций, которые используют вирусы для своего размножения и порчи информационных и программных ресурсов в компьютере, в том числе для переформатирования жесткого диска. Среди них можно выделить попытки изменения атрибутов файлов, коррекции исполняемых COM– или EXE-файлов, записи в загрузочные секторы диска.

При каждом запросе на подобное действие на экран компьютера поступает сообщение о том, какое действие затребовано, и какая программа будет его выполнять. В этом случае пользователь должен либо разрешить, либо запретить его исполнение. Постоянное нахождение программ-«сторожей» в ОП существенно уменьшает ее объем, что является основным недостатком этих программ. К тому же программы-фильтры не способны «лечить» файлы или диски. Эту функцию выполняют другие антивирусные программы, например AVP, Norton Antivirus for Windows, Thunder Byte Professional, McAfee Virus Scan.

*Программы-ревизоры* являются надежным средством защиты от вирусов. Они запоминают исходное состояние программ, каталогов и системных областей диска при условии, что компьютер еще не был заражен вирусом. Впоследствии программа периодически сравнивает текущее состояние с исходным. При обнаружении несоответствий (по длине файла, дате модификации, коду циклического контроля файла) сообщение об этом появляется на экране компьютера. Среди программ-ревизоров можно выделить программу Adinf и дополнение к ней в виде Adinf cure Module.

*Программа-доктор* способна не только обнаруживать, но и «лечить» зараженные программы или диски. При этом она уничтожает зараженные программы тела вируса. Программы данного типа можно разделить на фаги и полифаги. *Фаги* – это программы, с помощью которых отыскиваются вирусы определенного вида. *Полифаги* предназначены для обнаружения и уничтожения большого числа разнообразных вирусов. В нашей стране

наиболее часто используются такие полифаги, как MS Antivirus, Aidstest, Doctor Web. Они непрерывно обновляются для борьбы с появляющимися новыми вирусами.

*Программы-детекторы* способны обнаруживать файлы, зараженные одним или несколькими известными разработчикам программ вирусами.

*Программы-вакцины,* или *иммунизаторы,* относятся к классу резидентных программ. Они модифицируют программы и диски так, что это не отражается на их работе. Однако вирус, от которого производится вакцинация, считает их уже зараженными и не внедряется в них. В настоящий момент разработано множество антивирусных программ, получивших широкое признание и постоянно пополняющихся новыми средствами для борьбы с вирусами.

Программа-полифаг Doctor Web применяется для борьбы с полиморфными вирусами, появившимися сравнительно недавно. В режиме эвристического анализа эта программа эффективно определяет файлы, зараженные новыми, неизвестными вирусами. Используя *Doctor Web* для контроля дискет и получаемых по сети файлов, можно практически наверняка избежать заражения системы.

При использовании ОС Windows NT возникают проблемы с защитой от вирусов, созданных специально для этой среды. Также появилась новая разновидность инфекции – макровирусы, которые «вживляются» в документы, подготавливаемые текстовым процессором Word и электронными таблицами Excel. К наиболее распространенным антивирусным программам относятся AntiViral Toolkit Pro (AVP32), Norton Antivirus for Windows, Thunder Byte Professional, McAfee Virus Scan. Данные программы функционируют в режиме программ-сканеров и проводят антивирусный контроль ОП, папок и дисков. Кроме того, они содержат алгоритмы для распознавания новых типов вирусов и позволяют в процессе проверки лечить файлы и диски.

Программа AntiViral Toolkit Pro (AVP32) представляет собой 32-разрядное приложение, работающее в Windows NT. Она имеет удобный

пользовательский интерфейс, систему помощи, гибкую систему настроек, выбираемых пользователем, распознает более 7 тыс. различных вирусов. Эта программа определяет (детектирует) и удаляет полиморфные вирусы, вирусы-мутанты и вирусы-невидимки, а также макровирусы, которые заражают документ Word и таблицы Excel, объекты Access – «троянские кони».

Важной особенностью этой программы является возможность контроля всех файловых операций в фоновом режиме и обнаружения вирусов до момента реального заражения системы, а также детектирования вирусов внутри архивов формата ZIP, ARJ, ZHA, RAR.

Интерфейс программы AllMicro Antivirus является простым. Она не требует от пользователя дополнительных знаний о продукте. При работе с данной программой следует нажать кнопку Пуск (Scan), после чего начнется проверка или сканирование ОП, загрузочных и системных секторов жесткого диска, а затем и всех файлов, включая архивные и упакованные.

Программа Vscan 95 при начальной загрузке проверяет память компьютера, загрузочные секторы системного диска и все файлы в корневом каталоге. Две остальные программы пакета (McAfee Vshield, Vscan) являются приложениями Windows. Первая после загрузки Windows используется для слежения за вновь подключенными дисками, контроля исполняемых программ и копируемых файлов, а вторая – для дополнительной проверки памяти, дисков и файлов. Пакет McAfee VirusScan способен находить макровирусы в файлах MS Word.

В процессе развития локальных компьютерных сетей, электронной почты и сети Интернет и внедрения сетевой ОС Windows NT разработчиками антивирусных программ подготовлены и поставляются на рынок такие программы, как Mail Checker, позволяющая проверять входящую и исходящую электронную почту, и AntiViral Toolkit Pro для Novell NetWare (AVPN), применяемая для обнаружения, лечения, удаления и перемещения в специальный каталог пораженных вирусом файлов. Программа AVPN используется как антивирусный сканер и фильтр, который постоянно

контролирует хранящиеся на сервере файлы. Он способен удалять, перемещать и «лечить» пораженные объекты; проверять упакованные и архивные файлы; определять неизвестные вирусы с помощью эвристического механизма; проверять в режиме сканера удаленные серверы; отключать зараженную станцию от сети. Программа AVPN без труда настраивается для сканирования файлов различных типов и имеет удобную схему пополнения антивирусной базы.

### 10.7. Защита программных продуктов

Программные продукты являются важными объектами защиты по целому ряду причин:

1) они представляют собой продукт интеллектуального труда специалистов высокой квалификации, или даже групп из нескольких десятков или даже сотен человек;

2) проектирование этих продуктов связано с потреблением значительных материальных и трудовых ресурсов и основано на применении дорогостоящего компьютерного оборудования и наукоемких технологий;

3) для восстановления нарушенного программного обеспечения необходимы значительные трудозатраты, а применение простого вычислительного оборудования чревато негативными результатами для организаций или физических лиц.

Защита программных продуктов преследует следующие цели:

• ограничение несанкционированного доступа отдельных категорий пользователей к работе с ними;

• исключение преднамеренной порчи программ с целью нарушения нормального хода обработки данных;

• недопущение преднамеренной модификации программы с целью порчи репутации производителя программной продукции;

• препятствование несанкционированному тиражированию (копированию) программ;

• исключение несанкционированного изучения содержания, структуры и механизма работы программы.

Программные продукты следует защищать от несанкционированных воздействий различных объектов: человека, технических средств, специализированных программ, окружающей среды. Влияние на программный продукт возможно через применение хищения или физического уничтожения документации на программу или самого машинного носителя, а также путем нарушения работоспособности программных средств.

Технические средства (аппаратура) через подключение к компьютеру или передающей среде могут осуществить считывание, расшифровку программ, а также их физическое разрушение.

Заражение вирусом можно выполнить с помощью специализированных программ, вирусного заражения программного продукта, его несанкционированного копирования, недозволенного изучения его содержания.

Окружающая среда из-за аномальных явлений (повышенного электромагнитного излучения, пожара, наводнений) может быть причиной физического разрушения программного продукта.

Самый простой и доступный способ защиты программных продуктов заключается в ограничении доступа к ним с помощью:

• парольной защиты программ при их запуске;

• ключевой дискеты;

• специального технического устройства (электронного ключа), подключаемого к порту ввода-вывода компьютера.

Для того чтобы избежать несанкционированного копирования программ, специальные программные средства защиты должны:

• идентифицировать среду, из которой программа запускается;

• вести учет числа выполненных санкционированных инсталляций или копирования;

• противодействовать (вплоть до саморазрушения) изучению алгоритмов и программ работы системы.

Для программных продуктов действенными защитными мерами являются:

1) идентификация среды, из которой запускается программа;

2) ввод учета числа выполненных санкционированных инсталляций или копирования;

3) противодействие нестандартному форматированию запускающей дискеты;

4) закрепление месторасположения программы на жестком диске;

5) привязка к электронному ключу, вставляемому в порт ввода-вывода;

6) привязка к номеру BIOS.

При защите программных продуктов необходимо использовать и правовые методы. Среди них выделяются лицензирование соглашений и договоров, патентная защита, авторские права, технологическая и производственная секретность.

**10.8. Обеспечение безопасности данных на автономном компьютере**

Самыми типичными случаями, создающими угрозу данным, являются случайное стирание данных, отказ программного обеспечения и аппаратные сбои. Одна из первых рекомендаций пользователю состоит в резервировании данных.

Для магнитных дисков имеется такой параметр, как среднее время между отказами. Он может быть выражен в годах, поэтому необходимо резервное копирование.

При работе на компьютере данные иногда не читаются из-за выхода из строя платы управления жестким диском. При замене платы контроллера и перезагрузке компьютера можно вновь выполнять прерванную работу.

Для того чтобы обеспечить сохранность данных, необходимо создавать резервные копии. Применение копирования как одного из методов обеспечения безопасности данных требует выбора программного продукта,

процедуры (полное, частичное или выборочное копирование) и частоты резервного копирования. В зависимости от значимости информации иногда производят дубль-резервное копирование. Не следует пренебрегать и тестированием резервных копий. Данные необходимо защищать и в случае работы компьютера в малой сети, когда пользователи используют общие ресурсы файлового сервера.

К методам обеспечения безопасности относят:

• использование атрибутов файлов и каталогов типа «скрытый», «только для чтения»;

• сохранение важных данных на гибких магнитных дисках;

• помещение данных в защищенные паролем архивные файлы;

• включение в защитную программу регулярной проверки на компьютерные вирусы.

Существует три основных способа применения антивирусных программ:

1) поиск вируса при начальной загрузке, когда команда запуска антивирусной программы включается в AUTOEXEC.bat;

2) запуск вирусной программы вручную;

3) визуальный просмотр каждого загружаемого файла.

Прагматичным методом обеспечения безопасности информации на автономном компьютере является парольная защита. После включения компьютера и запуска программы установки CM08 пользователь может дважды ввести информацию, которая становится паролем. Далее защита на уровне CMOS блокирует компьютер целиком, если не введен правильный пароль.

В случае когда применение пароля нежелательно при начальной загрузке, некоторые модели клавиатуры можно заблокировать с помощью физических ключей, поставляемых в комплекте с компьютером.

Возможность защиты некоторых файлов предусматривается при работе пользователя с офисными пакетами (текстовыми процессорами,

электронными таблицами, СУБД) и выполнении команды сохранения файлов (Сохранить как...). Если в данном случае нажать на кнопку Options (Параметры), то в открывшемся диалоговом окне можно задать пароль, ограничивающий возможности работы с этим документом. Для того чтобы восстановить первоначальную форму защищенных таким образом данных, следует ввести тот же самый пароль. Пользователь может забыть либо, записав его на бумажном носителе, элементарно потерять пароль, тогда могут возникнуть еще большие неприятности, чем при работе без парольной защиты.

Способы защиты компьютеров, работающих автономно или в составе небольшой сети, дома или в офисе, достаточно разнообразны. При выборе стратегии защиты информации на компьютере надо найти компромисс между ценностью защищаемых данных, затратами на обеспечение защиты и неудобствами, которые налагаются системой защиты на работу с данными.

### 10.9. Безопасность данных в интерактивной среде

Интерактивные среды уязвимы с позиций безопасности данных. Примером интерактивных сред является любая из систем с коммуникационными возможностями, например электронная почта, компьютерные сети, Интернет.

*Электронная почта* представляет собой любой вид связи, используемый компьютерами и модемами. К наиболее незащищенным местам в электронной почте относятся пункт исходящей почты отправителя и почтовый ящик получателя. Каждый из программных пакетов электронной почты позволяет архивировать входящие и исходящие сообщения по любому другому адресу, что может привести к злоупотреблению злоумышленниками.

Электронная почта при обеспечении пересылки сообщений способна принести значительный вред получателю сообщений. Для предотвращения нежелательных последствий следует использовать и другие приемы безопасности, в том числе:

• нельзя сразу запускать программы, полученные по электронной почте, особенно вложения. Необходимо сохранить файл на диске, проверить его антивирусной программой и только затем запускать;

• запрещается сообщать свой пароль и личные данные, даже если отправитель предлагает адресату нечто очень заманчивое;

• при открытии полученных файлов MC Office (в Word, Excel) следует по возможности не использовать макросы;

• важно стараться применять проверенные, а также более новые версии почтовых программ.

Одной из важных проблем для пользователей Интернет является проблема безопасности данных в самой сети. Подключение пользователя к ресурсам производится через провайдера. С целью защиты информации от хулиганствующих элементов, неквалифицированных пользователей и преступников в системе Интернет применяется система полномочий, или управление доступом. Каждый файл данных (или другие ресурсы компьютера) обладает набором атрибутов, которые сообщают, что данный файл может просмотреть кто угодно, но изменять его имеет право лишь владелец. Еще одна проблема заключается в том, что никто, кроме владельца, не может просмотреть файл, несмотря на то что видны имена этих информационных ресурсов. Обычно пользователь стремится каким-то образом защитить свою информацию, но необходимо помнить, что системные администраторы могут преодолеть системы защиты. В данном случае на помощь приходят разнообразные методы шифрования информации с использованием ключей, разработанных пользователем.

Одной из проблем работы в сети Интернет является ограничение доступа некоторых категорий пользователей к информационным ресурсам (детей и школьников). Осуществить это можно с помощью специальных программных продуктов – брандмауэров (Net Nanny, Surf-Watch, Cyber Patrol). Они основываются на принципе фильтрации по ключевым словам, фиксированным спискам мест служб WWW, в которых находится

нежелательный для детей материал. Программы аналогичного вида, ведущие запись сеансов Интернет и отказывающие в доступе к определенным местам сети, могут устанавливаться в офисных и других учреждениях для предотвращения явления траты работниками времени в личных интересах.

Интернет – система, в которой многочисленные пользователи имеют свои Web-серверы, содержащие рекламную или справочную информацию на Web-страницах. Конкуренты способны испортить из содержание. Во избежание неприятностей в таких ситуациях можно регулярно просматривать Web-странички. При обнаружении порчи информации необходимо восстанавливать ее с помощью заранее заготовленных копий файлов. Важно иметь в виду, что обеспечивать безопасность информации на серверах обязаны провайдеры, которые систематически просматривают протоколы событий и обновляют программное обеспечение, если в нем обнаруживаются проблемы в защите.