Информационной безопасности сейчас уделяют большое внимание. В ряде вузов введены или вводятся новые специальности, связанные с под готовкой кадров по проблематике информационной безопасности. Вместе с тем, важно, чтобы всякий специалист, занимающийся разработкой вычисли тельной техники или программного обеспечения, или просто использующий ее в качестве пользователя, был знаком с проблемами информационной безопасности.

ВВЕДЕНИЕ

Общепринято, что развитие цивилизации тесно связано с информатизацией общества. Растущие потоки информации являются следствием развития общества и, в свою очередь, существенно влияют на его дальнейшее продвижение.

Тяга к знаниям, к получению все новых порций ин формации присуще человеку, а его право на получение информации нашло свое отражение в международном законодательстве. В «Декларации прав и свобод человека и гражданина», ратифицированной Верховным Советом Российской Федерации 22 ноября

11 года говорится: «Каждый имеет право искать, получать и свободно распространять информацию» [1].

Отчего же тогда надо защищать информацию? От метим, во первых, что все большие объемы информации обрабатываются с помощью автоматизированных систем обработки информации. Сложность таких систем растет. Вместе с тем ряд сбоев или отказов в функционировании таких систем могут привести к уничтожению информации или ее искажению. Так, например, выход из строя накопителя на жестком магнитном диске файлового сервера автоматизированной системы об работки информации банка может привести к катастрофическим последствиям, если не были приняты меры по сохранению хранившейся на диске информации.

Однако центральное место в проблеме защиты ин формации занимает преднамеренная деятельность людей, связанная с манипуляцией информацией, хранимой и обрабатываемой в автоматизированных системах в условиях бесконтрольного допуска к ней. В первую очередь это относится к случаям компьютерных преступлений, связанных с корыстным использованием и искажением информации, навязыванием ложных сообщений. Ряд других, возникающих здесь проблем, проиллюстрируем примерами.

К одному из наиболее характерных случаев вмешательства в работу вычислительных сетей относится поражение в 188 году сети InterNet вирусом (точнее червем) Морриса [2]. Сеть Internet объединяла в ту пору 1200 сетей, охватывающих 85200 узловых компьютеров, не только на территории США, но и в других странах Запада. В течение трех дней вирусом были инфицированы 6200 машин. Поражены были вычислительные центры Корнельского (НьЙорк), Стэнфордского (Калифорния), Принстонского (Нью Джерси) и ряда других университетов, вычислительные центры подсети MilNet (Military Net), объединяющих ряд исследовательских институтов и лабораторий, работающих на Министерство обороны США: Rand Corporation, Ливерморская лаборатория им. Лоуренса, Исследовательский центр НАСА, Армейская лаборатория баллистики и многие другие. Общие подсчитанные потери от вируса, созданного и запущенного студентом, составил около 100 млн. долларов. К расследованию этого случая было подключено ФБР. К счастью, вирус, блокируя работу практически всей сети Internet, не портил ин формацию, хранившуюся и обрабатываемую в сети. Тем не менее, по характеру последствий данный случай был расценен как национальная катастрофа. Результаты исследований действия вируса и выбора необходимых мер по ликвидации последствий были быстро засекречены, публикации, посвященные этому случаю, прекратились.

Другим моментом, связанным с компьютерными преступлениями, является нарушение авторских прав на программное обеспечение. Проблема незаконного копирования и использования программного обеспечения характерна не только для России. Доля “пиратского” программного продукта в общем объеме используемого программного обеспечения (ПО) колеблется от 50% в развитых странах до 05% — в неразвитых. По имеющимся оценкам убытки от несанкционированного копирования программ составляют в США около 50% от стоимости общего рынка про грамм. Для нас эта проблема важна тем, что широкое использование незаконно приобретенного программного обеспечения подрывает отечественную индустрию программного обеспечения.

Для характеристики состояния дела у нас в России ограничимся только оценкой Председателя Госте комиссии при Президенте РФ: «...Отсталость информационных технологий, не обеспечивающих защиту ин формации, высокая скрытность преступлений, совершаемых с помощью компьютерных средств, сложность их доказательства, создают благоприятные условия для развития в России информационной преступности. Как показали проверки банков, уже в

11–2 г.г. в стране совершен ряд преступлений в ин формационной сфере. Общий ущерб от них составил несколько десятков миллиардов рублей и имеет устойчивую тенденцию к дальнейшему росту».

Приведенные примеры относятся хотя и к недалекому, но прошлому. За прошедшее время можно было учесть уроки происшедшего и принять меры, предотвращающие несанкционированный доступ к информации, хранимой и обрабатываемой в вычислительных системах. Однако ситуация не становится существенно лучшей.

Из изложенного следует, что для обеспечения нормального функционирования информационных систем всех уровней необходимо озаботиться тем, как:

* Предотвратить разрушительное вторжение в систему;
* из общего объема хранимой и обрабатываемой ин формации выделить некоторую часть ее, которая не должна быть общедоступной;
* Своевременно и в полном объеме обеспечить пре доставление необходимой информации законному пользователю.

Наряду с названными проблемами, решение которых обеспечивает защиту информации, в последнее время все большее внимание уделяется также проблемам защиты пользователя от “вредной” информации. Вредные воздействия на пользователя могут носить различный характер. Говоря, например, о влиянии “виртуальной реальности” на психику человека, имеют в виду некоторые неисследованные технические и медицинские аспекты. На другом полюсе стоят проблемы, связанные со злонамеренными или корыстны ми устремлениями некоторых представителей общества. Сюда можно отнести лживую рекламу, пропаганду насилия, и т.п.

Понятия “защита информации” и “защита от ин формации” аккумулируют в себе понятие “информационная безопасность”.

Информация и информатизационные процессы стали неотъемлемой частью жизни личности, общества и государства, а информационная безопасность значимой составляющей национальной безопасности.

1. ОТ ЧЕГО НАДО ЗАЩИЩАТЬ ИНФОРМАЦИЮ Для того чтобы сформулировать задачи защиты ин формации от злоумышленников, необходимо пред ставить себе их цели и возможности по достижению этих целей.

Обычно различают следующие цели нарушителя:

* незаконное завладение конфиденциальной информацией;
* искажение информации;
* уничтожение информации;
* нарушение функционирования АС;
* незаконное копирование программ(и другой цен ной информации);
* отказ от информации.

Под конфиденциальной информацией будем понимать информацию, 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.

Искажение информации также может быть явным или неявным для владельца информации. Если, к примеру, злоумышленник перехватил (шифрованное) сообщение и не может узнать его содержания, он может произвольно исказить часть текста. Скорее всего, получатель обнаружит такое искажение и предпримет меры по исправлению ситуации. Неявное искажение информации называют модификацией. Модификация информации может проявляться по разному. На пример, в финансовом документе она может заключаться в “исправлении” номера счета, куда надо пере слать 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 по рядка 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. Следствием такого нарушения может быть непредставление информации законному пользователю. Нарушения функционирования АС 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 на 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 по лучив 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 компьютерных и сетевых технологий.

2. УЯЗВИМЫЕ МЕСТА В АВТОМАТИЗИРОВАН НЫХ СИСТЕМАХ И СЕТЯХ

Перечисляя уязвимые места автоматизированных систем и сетей с точки зрения защиты информации, мы вынуждены будем перечислить практически все эле менты, их составляющие.

1. Рассмотрим отдельную автоматизированную систему, представляющую собой отдельный компьютер или локально вычислительную сеть. Иногда для краткости будем называть ее просто системой.

Если злоумышленник получил доступ к компьютеру с защищаемой информацией, то он может ее скопировать, изменить или уничтожить. Кроме тог, нарушитель может вывести компьютер из строя или предпринять действия по нарушению функционирования автоматизированной системы, элементом которой он является.

При наличии в автоматизированной системе информации ограниченного доступа для ее защиты обычно формулируются и реализуются правила разграничения доступа. Впрочем, в соответствии с Федеральным законом “Об информации, информатизации и защите информации” защите, (по меньшей мере — защите от уничтожения), должна подлежать любая информация, входящая в состав информационного ресурса, или являющаяся собственностью либо товаром. Поэтому правила разграничения доступа должны быть сформулированы всегда. Их минимальным содержанием должно быть различение пользователей по принципу “свой — чужой”. Действия злоумышленника по получению доступа к информации в обход правил разграничения доступа (с использованием только штатных средств вычислительной системы) носят название несанкционированного доступа.

2. Рассмотрим теперь автоматизированную систему в составе телекоммуникационной сети. Даже если она защищена от несанкционированного доступа к информации, она может быть уязвима от злоумышленника, имеющего удаленный доступ. Более того, удаленный доступ может принести больший вред, чем несанкционированный доступ внутри системы. Дело в том, что в рассматриваемом случае злоумышленник может потратить на исследование возможности проникновения в систему значительное время и оставаться при этом анонимным. В результате проникновения он может достичь тех же целей, что и при локальном несанкционированном доступе: утечки, искажения и/или уничтожения информации. Он может попытаться нарушить функционирование системы, запустив решение своей, быть может бессмысленной задачи, требующей всех или почти всех ресурсов системы. Другими способами нарушения функционирования системы могут быть организация потока запросов, критичного по объему для системы, либо запуск вируса или червя. Наконец, именно в условиях удаленного доступа возможен отказ от факта отправления или факта получения сообщения.

3. Весьма уязвимы сети в случае получения злоумышленником доступа к узлу связи, а также при подключении к коммутационному оборудованию. В этих случаях злоумышленник получает возможность:

* считывать и модифицировать информацию, про ходящую через точку подключения;
* блокировать прохождение информации;
* записывать и посылать сообщения повторно;
* создавать и посылать свои сообщения, маскируя их под сообщения законных пользователей;
* наблюдать трафик (интенсивность и объемы обмена информацией, направления передачи информации).

4. Примерно такие же возможности имеются у злоумышленника, подключившегося к каналу связи. Однако сама такая возможность подключения зависит от

физической природы канала. Наиболее чувствительны к перехвату информации радиоканалы и, в том числе, каналы спутниковой связи. Подключение к ка налу связи в этом случае производится с использованием антенны и соответствующего связного оборудования. Подключение остается практически незаметным для законных пользователей сети.

Съем информации с кабельных каналов, даже оптоволоконных, также возможен, хотя и более сложен, чем в случае использования радиоканалов.

5. Компьютер и его составные части: системный блок, дисплей, клавиатура — являются элементами электронного оборудования. Происходящие в них физические процессы во время функционирования, при водят к возникновению переменных электромагнитных полей. Указанные поля могут нести в себе защищаемую информацию ограниченного доступа. Эта ин формация может улавливаться специальными приемными устройствами на некотором удалении от компьютера. В данном случае говорят об уязвимости от паразитных электромагнитных излучений.

При определенных условиях утечка информации может быть организована по акустическому, оптическому, вибрационному каналам. В общем случае говорят об уязвимости к утечке информации по техническим каналам утечки.

3. НАПРАВЛЕНИЯ ЗАЩИТЫ ИНФОРМАЦИИ Анализ уязвимых мест автоматизированных систем обработки информации, а также возможностей злоумышленника по воздействию на автоматизированную систему, дает возможность выделить несколько относительно самостоятельных направлений защиты информации. К ним относятся:

* законодательное обеспечение защиты информации;
* защита информации от несанкционированного до ступа;
* развитие и использование криптографических методов защиты информации;
* защита информации от компьютерных вирусов и других опасных воздействий по каналам распространения программ;
* защита от несанкционированного копирования и распространения программ и ценной компьютер ной информации;
* защита конфиденциальной информации от утечки по каналам побочных электромагнитных излучений и наводок;
* защита информации в чрезвычайных ситуациях и при неисправности аппаратной части АС.

3.1. ЗАКОНОДАТЕЛЬНОЕ ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ИНФОРМАЦИИ.

Концептуальные вопросы обеспечения информационной безопасности в Российской Федерации определяются Законом Российской Федерации №24461 от

5 марта 12 года “О безопасности”, Концепцией национальной безопасности Российской Федерации, и Доктриной информационной безопасности, которая утверждена Президентом Российской Федерации сентября 2000 года [11].

Действующим законодательством Российской Федерации определяется правовой статус информации, конституционные права граждан в области информационной безопасности, правовые основы защиты ин формации ограниченного доступа и защиты интеллектуальной собственности.

Ряд подзаконных нормативных документов определяет системы лицензирования деятельности по за щите информации и сертификации средств защиты информации. Ввиду исключительной важности ин формации и информатизации для развития общества и государства.

3.2. ЗАЩИТА ИНФОРМАЦИИ

ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

Защита информации от НСД решает следующие задачи [12]:

* защита информации ограниченного доступа от утечки;
* защита информации от искажения (обеспечение целостности информации);
* защита автоматизированной системы от попыток нарушения ее функционирования.

В части технической реализации защита от НСД сводится к задаче разграничения функциональных полномочий и доступа к информации.

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.

Организация защиты информации от НСД предусматривает наличие механизмов аутентификации (подтверждения подлинности):

субъекта доступа (локального или удаленного);

содержания получаемого сообщения;

текущего сеанса связи.

Наиболее известной системой аутентификации субъекта локального доступа является парольная система.. Существующее многообразие программно-аппаратных средств аутентификации требуют использования аутентификаторов, представляющих собой либо некий личный секрет (например ключевая дискета, электронный ключ), либо уникальный не подделываемый признак (например, отпечаток пальца, радужная оболочка глаза).

В случае удаленного доступа для аутентификации отправителя, содержания сообщения и сеанса связи чаще всего используется электронная цифровая подпись.

Субъект доступа, успешно прошедший этап аутентификации получает доступ к ресурсам в соответствии с правилами разграничения доступа. Правила разграничения доступа должны четко указывать каждому субъекту доступа объекты, доступные для него (файлы, папки, и т.п.) и права на их использование: создавать, читать, редактировать, удалять, и т.п.

3.3. ИСПОЛЬЗОВАНИЕ КРИПТОГРАФИЧЕСКИХ МЕТОДОВ ЗАЩИТЫ ИНФОРМАЦИИ

Стержень любой системы защиты — криптографические средства.

Как наука, а иногда и как искусство шифрования сообщений, криптография имеет многовековую историю. Развитие компьютерных систем телекоммуникаций, необходимость решения задач аутентификации и ряда других задач, связанных с обеспечением юридической значимости электронных документов и защитой от отказов привели в последнее время к развитию новых направлений в криптографии, связанных с решением такого рода задач [6, 14].

1. Под шифрованием информации понимают такое ее преобразование, при котором противник или злоумышленник, получив доступ к такой преобразован ной информации, не сможет ничего понять.

Система шифрованного обмена информацией вы глядит следующим образом. Отправитель сообщения шифрует открытый текст на некотором секретном ключе, получает шифрованный текст, или крипто грамму, и посылает ее по каналу связи. Получатель на некотором секретном ключе расшифровывает шифрованный текст и получает открытый текст сообщения. Третья заинтересованная сторона — противник, или злоумышленник, перехватив криптограмму, пытается дешифровать ее, то есть определить тем или иным способом открытый текст сообщения или секретный ключ.

2. Все криптографические системы подразделяются на два класса.

Классические или симметричные системы, характеризуются тем, что ключ для зашифрования совпадает с ключом расшифрования, и, следовательно, является секретным. Одинаковыми ключами отправителя и получателя, как правило, снабжает третья сторона — служба генерации и рассылки ключей.

Асимметричные криптосистемы возникли из потребности организации шифрованного обмена информацией в сетях ЭВМ в условиях отсутствия служб централизованного изготовления и рассылки ключей. При использовании асимметричной системы потенциальный получатель секретной информации выбирает (или вычисляет по известному алгоритму) ключ, который держит в секрете и будет использовать его для расшифрования получаемых им сообщений. Да лее, он вычисляет парный секретному ключ для зашифрования сообщений. Этот ключ не является секрет ным, объявляется общедоступным (public key), и публикуется или рассылается предполагаемым отравителям сообщений.

Асимметричные шифры работают с заметным замедлением по сравнению с симметричными шифрами. Поэтому в настоящее время наиболее перспективным представляются решения, связанные с гибридными криптосхемами, использующими традиционные методы шифрования с секретным ключом для защиты сек ретности и целостности, при одновременном использовании методов шифрования с открытым ключом для реализации функций распределения ключей.

Использование симметричных криптографических систем позволяют решать проблемы аутентификации и обеспечения целостности сообщения. Аутентификация отправителя достигается самим фактом получения сообщения, зашифрованного на ключе, известном только отправителю. Проверка целостности сообщения обеспечивается добавлением в текст криптограммы некоторой дополнительной информации (имитовставки), играющей роль контрольной суммы. Контрольная сумма является функцией всего сообщения и секретного ключа. Целостность сообщения подтверждается совпадением значений контрольной суммы, вычисленной на передающем и приемном концах.

Описанная система подтверждения целостности сообщения хорошо работает в условиях взаимодоверия среди участников обмена. Для аутентификации информации при отсутствии взаимного доверия между участниками информационного обмена Диффи и Хэлманом в 176 году была предложена концепция

«цифровой подписи».[13] Она заключается в использовании асимметричных криптосистем для аутентификации информации.

Цифровая подпись вычисляется на основе текста подписываемого сообщения и секретного личного ключа. Всякий желающий убедиться в подлинности сообщения использует для этого в качестве проверочной комбинации общедоступный ключ. При этом знание проверочной комбинации не дает возможности подделать подпись.

Таким образом, составными частями, обеспечивающими реализацию цифровой подписи являются:

* генерация секретного ключа с помощью датчика случайных ключей;
* выработка и опубликование открытого ключа;
* формирование подписи;
  + - проверка подписи.

Самой важной характеристикой используемых криптографических систем является их стойкость, определяющая уверенность в том, что предполагаемый злоумышленник, не имеющий доступа к используемому криптографическому ключу, не сможет де шифровать и понять смысл перехваченной шифрованной информации, либо имитировать подпись хотя бы одного сообщения. Проведение исследований, позволяющих получить такую оценку, являются весьма трудоемким и дорогостоящим делом, посильным только профессиональным криптографам. Поэтому на практике рекомендуется использовать только сертифицированные криптографические средства, про шедшие всесторонние исследования и аттестацию ФАПСИ. В качестве примера гарантированно стой кого алгоритма шифрования можно привести алгоритм по ГОСТ 281478.

3.4. ЗАЩИТА ОТ ВИРУСОВ И ЗАКЛАДОК

Защита информации от компьютерных вирусов и других опасных воздействий по каналам распространения программ актуальна ввиду больших масштабов

«вирусных эпидемий», при которых заражаются сот ни тысяч компьютеров.

В последнее время все чаще среди специалистов упоминают об информационном оружии. Одним из элементов такого оружия является внедрение в защищаемые системы специальных программ, называемых программными закладками. Такие закладки могут быть нацелены на нейтрализацию штатных средств защиты от НСД, нарушение функционирования автоматизированной системы, копировании и негласной передачи, как смысловой информации (данных), так и паролей.

Как правило, рассматриваются два направления в методах защиты от программ с вредным воздействием [15, 16]:

* применение «иммунно-стойких» программных средств, защищенных от возможности несанкционированной модификации (разграничение доступа, методы самоконтроля и самовосстановления);
* применение специальных программ анализаторов, осуществляющих постоянный контроль возникновения «аномалий» в деятельности прикладных программ, периодическую проверку наличия других возможных следов вирусной активности (на пример, обнаружение нарушений целостности программного обеспечения), а также «входной» контроль новых программ перед их использованием (по характерным признакам наличия в их теле вирусных образований).

3.5. ЗАЩИТА ПРОГРАММ ОТ НЕСАНКЦИОНИРО" ВАННОГО КОПИРОВАНИЯ И ИСПОЛЬЗОВАНИЯ

1. Защита от несанкционированного копирования и распространения программ и ценной компьютерной информации ориентирована на проблему охраны интеллектуальной собственности, воплощенной в виде программ и ценных баз данных. Такая защита обычно осуществляется с помощью специальных программных и/или программно-аппаратных средств, делающих неработоспособной нелегальную копию программы. [17–20]

Программы, распространяемые на коммерческой основе, поставляются на сменных дисках. Реже — устанавливаются поставщиком на конкретный компьютер. Идея, реализующая защиту от несанкционированного копирования заключается в том, чтобы создать

такой дистрибутив, что копия с него, получаемая штатными средствами операционной системы, была бы неработоспособной. Для этого на дискете помимо блока с защищаемой информацией размещается блок не дублируемой оригинальной информации. Во время запуска программы и/или ее работы происходит обращение к не дублируемому блоку. При этом еще один блок программного обеспечения — блок сравнения, убеждается в наличии или отсутствии блока не дублируемой информации. По результатам сравнения либо подается команда на продолжение работы защищаемой программы, либо управление передается на блок реагирования. В качестве вариантов реакции в последнем случае могут быть команды прекращения работы программы, самоуничтожения защищаемого программного продукта и даже деструктивного воз действия на программную среду компьютера.

Наибольшее число методов создания не копируемых модулей связано с нестандартным форматированием дискет. Нестандартное форматирование осуществляется специальными контроллерами.

2. Широкое распространение получили программ но аппаратные средства защиты от несанкционированного копирования с использованием электронных ключей.

Электронные ключи — это компактные устройства, которые подключаются к одному из внешних разъемов компьютера, «прозрачные» для периферийных устройств и играют роль блока не дублируемой оригинальной информации. Для реализации этой цели электронные ключи выполняются со значительными функциональными возможностями, включающими в себе возможность изменения внутреннего со стояния. Через один разъем можно подключить не сколько электронных ключей, каждый из которых обеспечивает защиту своей программы. Одновремен но через этот разъем может осуществляться интерфейс с принтером.

3. Противодействие восстановлению алгоритмов. При невозможности получения несанкционированной копии защищаемой дискеты достаточно просты ми методами злоумышленник может попытаться восстановить защищаемую программу или алгоритм, ре ализуемый защищаемой программой. Восстановление программы или алгоритма возможно двумя способа ми. Первый из них связан с анализом и последующим дисассемблированием распечатки всего программного обеспечения, имеющегося на дискете. В этом случае говорят о статических методах анализа программ. Во втором случае исследуют алгоритм работы программы, запуская ее под отладчиком в пошаговом режиме и фиксируя выполняемые действия и переходы. В данном случае говорят о динамических методах анализа программ. Из изложенного следует, что защищаемое программное обеспечение должно содержать блоки противодействия статическому и динамическому анализам программ.

4. Проблеме защиты дискет от несанкционированного копирования посвящена многочисленная литература. Создано также значительное число программных и программно-аппаратных средств защиты от несанкционированного копирования. Однако надо отметить, что надежного решения этой проблемы нет. Любая защита от несанкционированного копирования вскрывается в конечное время [17]. Следовательно, при разработке средств защиты от не санкционированного копирования необходимо ста вить реальные задачи — затруднить потенциальному нарушителю незаконное использование программы, сделать невыгодным несанкционированное копирование.

3.6. ЗАЩИТА ИНФОРМАЦИИ ОТ УТЕЧКИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ

Данное направление базируется на предотвращении или существенном затруднении возможности получения нарушителем информации ограниченного доступа по каналам паразитных электромагнитных излучений и наводок (ПЭМИН), акустическим и другим техническим каналам за пределы охраняемой территории. При этом предполагается, что внутри охраняемой территории применяются эффективные режимные меры, исключающие возможность бесконтрольного использования специальной аппаратуры пере хвата, регистрации и отображения электромагнитных сигналов. Для защиты от ПЭМИН широко используются экранирование помещений, а также технические меры, позволяющие снизить интенсивность информативных излучений самого оборудования ЭВМ и связи. В последнее время определенное распространение получил метод электромагнитной маскировки информативных сигналов.

В некоторых ответственных случаях необходима дополнительная проверка вычислительного оборудования на предмет возможного выявления специальных закладных устройств промышленного шпионажа, которые могут быть внедрены недобросовестным конкурентом с целью ретрансляции или записи информативных излучений компьютера, а также речевых и других несущих уязвимую информацию сигналов [21].

3.7. ЗАЩИТА ИНФОРМАЦИИ

В ЧРЕЗВЫЧАЙНЫХ СИТУАЦИЯХ

И ПРИ НЕИСПРАВНОСТИ АППАРАТНОЙ ЧАСТИ АС

1. Чрезвычайные ситуации могут возникнуть в результате стихийных бедствий (землетрясения и т.п.), техногенных катастроф (пожары, взрывы и т.п.), террористических актов и военных действий.

Наиболее уязвимыми объектами обеспечения информационной безопасности в условиях чрезвычайных ситуаций являются система принятия решений по оперативным действиям, связанным с развитием таких ситуаций, и ходом ликвидации их по следствий.

В рассматриваемых условиях ценность информации такова, что она должна остаться в целости и доступности при разрушении здания, оборудования, и т.п.. Поэтому большое внимание должно уделяться резервному копированию. Резервные копии должны храниться в других помещениях, зданиях, или, даже, в других городах.

2. Перебои с питанием являются одной из первых причин потери информации в функционирующей вы числительной системе. При пропадании питания, даже на доли секунды, стирается информация, обрабатываемая в энергозависимой оперативной памяти. Средством защиты в рассматриваемом случае является использование источников непрерывного питания.

3. Угрозы потери информации от сбоев и неисправностей аппаратной части АС часто решаются испытанным средством — дублированием подвержен ной опасности части оборудования.

Близки по последствиям и угрозы, возникающие из-за ошибок в программном обеспечении. Нередки случаи, когда работа даже фирменного программного обеспечения в определенных ситуациях приводит к «зависанию» вычислительной системы. По следующий перезапуск приводит к потере информации, находящейся в оперативной памяти. Повышению надежности программного обеспечения может способствовать тщательное тестирование программного продукта по возможности во всех режимах его работы.

4. Причинами потери или искажения информации, передаваемой в сети, являются:

* сбои и неисправности сетевого оборудования;
* помехи в канале связи.

В локально вычислительных сетях значительна доля угроз за счет неисправностей в кабельном хозяйстве. В связи с этим рекомендуется иметь и использовать для выявления факта и места разрыва кабеля или короткого замыкания в нем специальные тестеры.

Для повышения надежности передачи информации в условиях помех используют коды, обнаруживающие и исправляющие ошибки.

5. Неопытность пользователя, ошибки оператора дают значительную долю случаев потери информации. Современное программное обеспечение, как в рамках операционной системы, так и в специальных утилитах, содержит средства, защищающие от ошибочного стирания информации даже в таких тяжелых случаях, как случайное форматирование дисков.

В заключение отметим, что при построении системы защиты информации необходим комплексный подход, учитывающий необходимость “закрытия” всех слабых мест вычислительной системы.