3. Угрозы информационной безопасности. Построение систем защиты от угрозы нарушения конфиденциальности информации. Защита информации от утечки по техническим каналам

3.1. Анализ уязвимостей системы

При построении системы защиты информации обязательно нужно определить, что следует защищать и от кого (или чего) следует строить защиту. Определение информации, подлежащей защите, было дано выше. Защищаться следует от множества угроз, которые проявляются через действия нарушителя. Угрозы возникают в случае наличия в системе уязвимостей, то есть таких свойств АС, которые могут привести к нарушению информационной безопасности.

Определение перечня угроз и построение модели нарушителя являются обязательным этапом проектирования системы защиты. Для каждой системы перечень наиболее вероятных угроз безопасности, а также характеристика наиболее вероятного нарушителя индивидуальны, поэтому перечень и модель должны носить неформальный характер. Защищенность информации обеспечивается только при соответствии предполагаемых угроз и качеств нарушителя реальной обстановке.

При наличии в системе уязвимости потенциальная угроза безопасности может реализоваться в виде атаки. Атаки принято классифицировать в зависимости от целей, мотивов, используемого механизма, места в архитектуре системы и местонахождения нарушителя.

Для предупреждения успешных атак необходим поиск и анализ уязвимостей системы. Уязвимости различаются в зависимости от источника возникновения, степени риска, распространенности, места в жизненном цикле системы, соотношения с подсистемами защиты АС. Анализ уязвимостей – обязательная процедура при аттестации объекта информатизации. В связи с возможностью появления новых уязвимостей, необходим их периодический анализ на уже аттестованном объекте.

3.2. Классификация угроз информационной безопасности

Угроза – это фактор, стремящийся нарушить работу системы.

В настоящее время рассматривается достаточно обширный перечень угроз информационной безопасности АС, насчитывающий сотни пунктов.

Кроме выявления возможных угроз должен быть проведен анализ этих угроз на основе их классификации по ряду признаков. Каждый из признаков классификации отражает одно из обобщенных требований к системе защиты. При этом угрозы, соответствующие каждому признаку классификации, позволяют детализировать отражаемое этим признаком требование.

Необходимость классификации угроз информационной безопасности АС обусловлена архитектурой современных средств автоматизированной обработки информации. Специфика ее такова, что накапливаемая, хранимая и обрабатываемая информация подвержена случайным влияниям чрезвычайно большого числа факторов, в силу чего становится невозможным описать полное множество угроз. Для защищаемой системы определяют не полный перечень угроз, а перечень классов угроз, определяемых по ряду базовых признаков [3].

Существует следующая классификация угроз информационной безопасности:

1. По природе возникновения.

1.1. Естественные угрозы, вызванные воздействиями на АС и ее компоненты объективных физических процессов или стихийных природных явлений, не зависящих от человека.

1.2. Искусственные угрозы информационной безопасности АС, вызванные деятельностью человека.

2. По степени преднамеренности проявления.

2.1. Угрозы случайного действия и/или угрозы, вызванные ошибками или халатностью персонала. Например, проявление ошибок программно-аппаратных средств АС, некомпетентное использование, настройка или неправомерное отключение средств защиты персоналом службы безопасности, неумышленное повреждение каналов связи.

2.2. Угрозы преднамеренного действия. Например, угрозы, вызванные действиями злоумышленника по хищению информации.

3. По непосредственному источнику угроз.

3.1. Угрозы, непосредственным источником которых является природная среда (стихийные бедствия, магнитные бури, радиоактивное излучение и т. п.).

3.2. Угрозы, непосредственным источником которых является человек. Например, разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных карточек, пропусков и т. п.).

3.3. Угрозы, непосредственным источником которых являются санкционированные программно-аппаратные средства. Например, запуск технологических программ, способных при некомпетентном использовании вызывать утрату работоспособности системы (зависания или зацикливания) или необратимые изменения в системе (форматирование или реструктуризацию носителей информации, удаление данных и т. п.).

3.4. Угрозы, непосредственным источником которых являются несанкционированные программно-аппаратные средства. Например, нелегальное внедрение и использование неучтенных программ (игровых, обучающих, технологических и других, не являющихся необходимыми для выполнения нарушителем своих служебных обязанностей) с последующим необоснованным расходованием ресурсов (загрузка процессора, захват оперативной памяти и памяти на внешних носителях), заражение компьютера вирусами с деструктивными функциями.

4. По положению источника угроз.

4.1. Угрозы, источник которых находится вне контролируемой зоны территории (помещения) с расположенной в ней АС. Например, перехват побочных электромагнитных излучений устройств и линий связи, перехват данных, передаваемых по каналам связи; дистанционная фото- и видеосъемка.

4.2 Угрозы, источник которых находится в пределах контролируемой зоны территории (помещения) с расположенной в ней АС. Например, хищение производственных отходов (распечаток, записей, списанных носителей информации и т. п.), применение подслушивающих устройств.

4.3. Угрозы, источник которых имеет доступ к периферийным устройствам АС (терминалам).

4.4. Угрозы, источник которых расположен в АС. Например, некорректное использование ресурсов АС.

5. По степени зависимости от активности АС.

5.1. Угрозы, которые могут проявляться независимо от активности АС. Например, вскрытие шифров криптозащиты информации, хищение носителей информации.

5.2. Угрозы, которые могут проявляться только в процессе автоматизированной обработки данных. Например, угрозы исполнения и распространения программных вирусов.

6. По степени воздействия на АС.

6.1. Пассивные угрозы, которые при реализации ничего не меняют в структуре и содержании АС. Например, угроза копирования секретных данных.

6.2. Активные угрозы, которые при воздействии вносят изменения в структуру и содержание АС. Например, внедрение аппаратных спецвложений, программных «закладок» и «вирусов» («троянских коней» и «жучков»), т. е. таких участков программ, которые не нужны для выполнения заявленных функций, но позволяют преодолеть систему защиты, скрытно и незаконно осуществить доступ к системным ресурсам с целью регистрации и передачи критической информации или дезорганизации функционирования системы.

7. По этапам доступа пользователей или программ к ресурсам АС.

7.1. Угрозы, которые могут проявляться на этапе доступа к ресурсам АС. Например, угрозы несанкционированного доступа в АС.

7.2. Угрозы, которые могут проявляться после разрешения доступа к ресурсам АС. Например, угрозы несанкционированного или некорректного использования ресурсов АС.

8. По способу доступа к ресурсам АС.

8.1. Угрозы, направленные на использование прямого стандартного пути доступа к ресурсам АС. Например, незаконное получение паролей и других реквизитов разграничения доступа (агентурным путем, используя халатность пользователей, подбором, имитацией интерфейса системы и т. д.)

8.2. Угрозы, направленные на использование скрытого нестандартного пути доступа к ресурсам АС. Например, вход в систему в обход средств защиты (загрузка посторонней операционной системы со сменных магнитных носителей и т. п.), угроза несанкционированного доступа к ресурсам АС путем использования недокументированных возможностей ОС.

9. По текущему месту расположения информации, хранимой и обрабатываемой в АС.

9.1. Угрозы доступа к информации на внешних запоминающих устройствах. Например, угроза несанкционированного копирования секретной информации с жесткого диска.

9.2. Угрозы доступа к информации в оперативной памяти. Например, чтение остаточной информации из оперативной памяти, угроза доступа к системной области оперативной памяти со стороны прикладных программ.

9.3. Угрозы доступа к информации, циркулирующей в линиях связи. Например, незаконное подключение к линиям связи с целью «работы между строк» с использованием пауз в действиях законного пользователя от его имени с последующим вводом ложных сообщений или модификацией передаваемых сообщений, перехват всего потока данных с целью дальнейшего анализа.

9.4. Угрозы доступа к информации, отображаемой на терминале или печатаемой на принтере. Например, угроза записи отображаемой информации на скрытую видеокамеру.

Вне зависимости от конкретных видов угроз или их проблемно-ориентированной классификации АС удовлетворяет потребности эксплуатирующих ее лиц, если обеспечиваются конфиденциальность, целостность и доступность информации.

Соответственно для автоматизированных систем было предложено рассматривать три основных вида угроз:

- *Угроза нарушения конфиденциальности* реализуется в том случае, если информация становится известной лицу, не располагающему полномочиями доступа к ней. Угроза нарушения конфиденциальности имеет место всякий раз, когда получен доступ к некоторой секретной информации, хранящейся в вычислительной системе или передаваемой от одной системы к другой. Иногда в связи с угрозой нарушения конфиденциальности используется термин «утечка».
- *Угроза нарушения целостности* реализуется при несанкционированном изменении информации, хранящейся в вычислительной системе или передаваемой из одной системы в другую. Когда злоумышленники преднамеренно изменяют информацию, говорится, что целостность информации нарушена. Целостность также будет нарушена, если к несанкционированному изменению приводит случайная ошибка программного или аппаратного обеспечения. Санкционированными изменениями являются те, которые сделаны уполномоченными лицами с обоснованной целью (например, санкционированным изменением является периодическая запланированная коррекция некоторой базы данных).
- *Угроза нарушения доступности* (отказа служб) реализуется, когда в результате преднамеренных действий, предпринимаемых другим пользователем или злоумышленником, блокируется доступ к некоторому ресурсу вычислительной системы. Блокирование может быть постоян-ным – запрашиваемый ресурс никогда не будет получен, или оно может вызывать только задержку запрашиваемого ресурса, достаточно долгую для того, чтобы он стал бесполезным.

Данные виды угроз можно считать первичными, или непосредственными, т. к. если рассматривать понятие угрозы как некоторой потенциальной опасности, реализация которой наносит ущерб информационной системе, то реализация вышеперечисленных угроз приведет к непосредственному воздействию на защищаемую информацию. В то же время непосредственное воздействие на информацию возможно для атакующей стороны в том случае,

если система, в которой циркулирует информация, для нее «прозрачна», т. е. не существует никаких систем защиты или других препятствий. Описанные выше угрозы были сформулированы в 60-х гг. применительно к открытым UNIX-подобным системам, для которых не предусматривались меры по защите информации.

На современном этапе развития информационных технологий подсистемы или функции защиты являются неотъемлемой частью комплексов по обработке информации. Информация не представляется «в чистом виде», на пути к ней имеется хотя бы какая-нибудь система защиты, и поэтому, чтобы угрожать, скажем, нарушением конфиденциальности, атакующая сторона должна преодолеть эту систему. Поскольку преодоление защиты также представляет собой угрозу, для защищенных систем будем рассматривать ее четвертый вид – *угрозу раскрытия параметров АС, включающей в себя систему защиты*. На практике любое проводимое мероприятие предваряется этапом разведки, в ходе которой определяются основные параметры системы, ее характеристики и т. п. Результатом разведки является уточнение поставленной задачи, а также выбор наиболее оптимального технического средства. Угрозу раскрытия параметров АС можно рассматривать как опосредованную. Последствия ее реализации не причиняют какой-либо ущерб обрабатываемой информации, но дают возможность реализоваться первичным, или непосредственным. угрозам, перечисленным выше. Введение данного вида угроз позволяет описывать с научно-методологической точки зрения отличия защищенных информационных систем от открытых. Для последних угроза разведки параметров системы считается реализованной.

3.2. Основные направления и методы реализации угроз

К **основным направлениям** реализации злоумышленником информационных угроз относятся [3]:

- непосредственное обращение к объектам доступа;
- создание программных и технических средств, выполняющих обращение к объектам доступа в обход средств защиты;
- модификация средств защиты, позволяющая реализовать угрозы информационной безопасности;
- внедрение в технические средства АС программных или технических механизмов, нарушающих предполагаемую структуру и функции АС.

К числу **основных методов** реализации угроз информационной безопасности АС относятся [3]:

- определение злоумышленником типа и параметров носителей информации;
- получение злоумышленником информации о программно-аппаратной среде, типе и параметрах средств вычислительной

техники, типе и версии операционной системы, составе прикладного программного обеспечения;

- получение злоумышленником детальной информации о функциях, выполняемых АС;
- получение злоумышленником данных о применяемых системах защиты;
- определение способа представления информации;
- определение злоумышленником содержания данных, обрабатываемых в АС, на качественном уровне (применяется для мониторинга АС и для дешифрования сообщений);
- хищение (копирование) машинных носителей информации, содержащих конфиденциальные данные;
- использование специальных технических средств для перехвата побочных электромагнитных излучений и наводок (ПЭМИН);
- уничтожение средств вычислительной техники и носителей информации;
- несанкционированный доступ пользователя к ресурсам АС в обход или путем преодоления систем защиты с использованием специальных средств, приемов, методов;
- несанкционированное превышение пользователем своих полномочий;
- несанкционированное копирование программного обеспечения;
- перехват данных, передаваемых по каналам связи;
- визуальное наблюдение;
- раскрытие представления информации (дешифрование данных);
- раскрытие содержания информации на семантическом уровне;
- уничтожение машинных носителей информации;
- внесение пользователем несанкционированных изменений в программно-аппаратные компоненты АС и обрабатываемые данные;
- установка и использование нештатного аппаратного и/или программного обеспечения;
- заражение программными вирусами;
- внесение искажений в представление данных, уничтожение данных на уровне представления, искажение информации при передаче по линиям связи;
- внедрение дезинформации;
- выведение из строя машинных носителей информации без уничтожения;

- проявление ошибок проектирования и разработки аппаратных и программных компонентов АС;
- искажение соответствия синтаксических и семантических конструкций языка;
- запрет на использование информации.

Перечисленные методы реализации угроз охватывают все уровни представления информации.

3.4. Неформальная модель нарушителя

Нарушитель – это лицо, предпринявшее попытку выполнения запрещенных операций (действий) по ошибке, незнанию или осознанно со злым умыслом (из корыстных интересов) или без такового (ради игры или удовольствия, с целью самоутверждения и т. п.) и использующее для этого различные возможности, методы и средства.

Злоумышленник – нарушитель, намеренно идущий на нарушение из корыстных побуждений.

Неформальная модель нарушителя отражает его практические и теоретические возможности, априорные знания, время и место действия и т. п. Исследовав причины нарушений, можно либо повлиять на сами эти причины, либо точнее определить требования к системе защиты от данного вида нарушений или преступлений.

В каждом конкретном случае исходя из конкретной технологии обработки информации может быть определена модель нарушителя, которая должна быть адекватна реальному нарушителю для данной АС.

Неформальная модель нарушителя разрабатывается при проектировании системы защиты и оценке защищенности информации.

При разработке модели нарушителя определяются:

- предположения о категориях лиц, к которым может принадлежать нарушитель;
- предположения о мотивах действий нарушителя (преследуемых нарушителем целях);
- предположения о квалификации нарушителя и его технической оснащенности (об используемых для совершения нарушения методах и средствах);
- ограничения и предположения о характере возможных действий нарушителей.

По отношению к АС нарушители могут быть внутренними (из числа персонала системы) или внешними (посторонними лицами). Практика показывает, что на долю внутренних нарушителей приходится более 2/3 от общего числа нарушений.

Внутренним нарушителем может быть лицо из следующих категорий персонала:

- пользователи (операторы) системы;
- персонал, обслуживающий технические средства (инженеры, техники);
- сотрудники отделов разработки и сопровождения ПО (прикладные и системные программисты);
- технический персонал, обслуживающий здания (уборщики, электрики, сантехники и другие сотрудники, имеющие доступ в здания и помещения, где расположены компоненты АС);
- сотрудники службы безопасности АС;
- руководители различных уровней должностной иерархии.

Посторонние лица, которые могут быть нарушителями:

- клиенты (представители организаций, граждане);
- посетители (приглашенные по какому-либо поводу);
- представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации (энерго-, водо-, теплоснабжения и т. п.);
- представители конкурирующих организаций (иностранных спецслужб) или лица, действующие по их заданию;
- лица, случайно или умышленно нарушившие пропускной режим (без цели нарушить безопасность АС);
- любые лица за пределами контролируемой территории.

Можно выделить три основных мотива нарушений: безответственность, самоутверждение и корыстный интерес.

При нарушениях, вызванных безответственностью, пользователь целенаправленно или случайно производит какие-либо разрушающие действия, не связанные тем не менее со злым умыслом. В большинстве случаев это следствие некомпетентности или небрежности. Даже если АС имеет средства, делающие такое проникновение чрезвычайно сложным, полностью защитить ее от проникновения практически невозможно.

Классификация нарушителей

По уровню знаний об АС:

- знает функциональные особенности АС, основные закономерности формирования в ней массивов данных и потоков запросов к ним, умеет пользоваться штатными средствами;

- обладает высоким уровнем знаний и опытом работы с техническими средствами системы, а также опытом их обслуживания;
- обладает высоким уровнем знаний в области программирования и вычислительной техники, проектирования и эксплуатации автоматизированных информационных систем;
- знает структуру, функции и механизм действия средств защиты, их сильные и слабые стороны.

По уровню возможностей (используемым методам и средствам):

Первый уровень определяет самый низкий уровень возможностей ведения диалога в АС запуск задач (программ) из фиксированного набора, реализующих заранее предусмотренные функции по обработке информации.

Второй уровень определяется возможностью создания и запуска собственных программ с новыми функциями по обработке информации.

Третий уровень определяется возможностью управления функционированием АС, т. е. воздействием на базовое программное обеспечение системы и на состав и конфигурацию ее оборудования.

Четвертый уровень определяется всем объемом возможностей лиц, осуществляющих проектирование, реализацию и ремонт технических средств АС, вплоть до включения в состав СВТ собственных технических средств с новыми функциями по обработке информации.

Классификация является иерархической, т. е. каждый следующий уровень включает в себя функциональные возможности предыдущего.

В своем уровне нарушитель является специалистом высшей квалификации, знает все о АС и, в частности, о системе и средствах ее защиты.

Классификация по уровню возможностей приводится в руководящем документе Гостехкомиссии «Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации» в разделе «Модель нарушителя в АС» [7].

По времени действия:

- в процессе функционирования АС (во время работы компонентов системы);
- в период неактивности компонентов системы (в нерабочее время, во время плановых перерывов в ее работе, перерывов для обслуживания и ремонта и т. п.);
- как в процессе функционирования АС, так и в период неактивности компонентов системы.

По месту действия:

- без доступа на контролируемую территорию организации;

- с контролируемой территории без доступа в здания и сооружения;
- внутри помещений, но без доступа к техническим средствам АС;
- с рабочих мест конечных пользователей (операторов) АС;
- с доступом в зону данных (баз данных, архивов и т.п.);
- с доступом в зону управления средствами обеспечения безопасности АС.

Определение конкретных характеристик возможных нарушителей в значительной степени субъективно. Модель нарушителя, построенная с учетом особенностей конкретной предметной области и технологии обработки информации, может быть представлена перечислением нескольких вариантов его облика. Каждый вид нарушителя должен быть определен с помощью характеристик, приведенных выше.

3.5. Методы оценки уязвимости системы

При решении практических задач защиты информации большое значение имеет количественная оценка ее уязвимости.

Ряд специалистов в области информационной безопасности выделяют методы и средства защиты от случайных и от преднамеренных угроз [5]. Для защиты от случайных угроз используются средства повышения надежности функционирования автоматизированных систем, средства повышения достоверности и резервирования информации.

При проектировании защиты от преднамеренных угроз определяются перечень и классификация по характеру, размещению, важности и времени жизни данных, подлежащих защите в заданной АС. В соответствии с характером и важностью этих данных выбираются ожидаемая квалификация и модель поведения потенциального нарушителя. Считается, что угроза реализуется путем несанкционированного доступа к информации.

В соответствии с моделью нарушителя в проектируемой системе выявляются виды и количество возможных каналов несанкционированного доступа к защищаемым данным. Данные каналы делятся на технически контролируемые и неконтролируемые [5]. Например, вход в систему со стороны клавиатуры терминала может контролироваться специальной программой, а каналы связи территориально-распределенной системы – не всегда. На основе анализа каналов выбираются готовые или создаются новые средства защиты с целью перекрытия этих каналов.

Для создания единого постоянно действующего механизма защиты средства защиты с помощью специально выделенных средств централизованного управления объединяются в одну автоматизированную систему безопасности информации, которая путем анализа ее состава и принципов построения проверяется на предмет наличия возможных путей ее обхода. Если таковые обнаруживаются, то они перекрываются

соответствующими средствами, которые также включаются в состав защитной оболочки. В результате будет построена замкнутая виртуальная оболочка защиты информации [5].

Степень защиты определяется полнотой перекрытия каналов утечки информации и возможных путей обхода средств защиты, а также прочностью защиты. Согласно принятой модели поведения нарушителя прочность защитной оболочки определяется средством защиты с наименьшим значением прочности из числа средств, составляющих эту оболочку.

Под *прочностью защиты* (преграды) понимается величина вероятности ее непреодоления нарушителем.

Прочность защитной преграды является достаточной, если ожидаемое время преодоления ее нарушителем больше времени жизни предмета защиты или больше времени обнаружения и блокировки доступа при отсутствии путей обхода этой преграды.

Защитная оболочка должна состоять из средств защиты, построенных по одному принципу (контроля или предупреждения НСД) и размещаемых на каналах НСД одного типа (технически контролируемых или неконтролируемых). На контролируемых каналах нарушитель рискует быть пойманным, а на неконтролируемых он может работать в комфортных условиях, не ограниченных временем и средствами. Прочность защиты во втором случае должна быть значительно выше. Поэтому целесообразно в автоматизированной системе иметь отдельные виртуальные защитные оболочки: контролируемую и превентивную.

Кроме того, необходимо учитывать применение организационных мероприятий, которые в совокупности могут образовать свою защитную оболочку.

Стратегия и тактика защиты от преднамеренного НСД заключается в применении на возможных каналах НСД к информации АС средств контроля, блокировки и предупреждения событий. Средства контроля и блокировки устанавливаются на возможных каналах НСД, где это возможно технически или организационно, а средства предупреждения (превентивные средства) применяются там, где такие возможности отсутствуют.

При расчете прочности средства защиты учитывается временной фактор, позволяющий получить количественную оценку его прочности – ожидаемую величину вероятности непреодоления его потенциальным нарушителем.

Рассмотрим варианты построения защитной оболочки и оценку ее прочности [5].

В простейшем случае предмет защиты помещен в замкнутую однородную защитную оболочку (рис. 3.1).

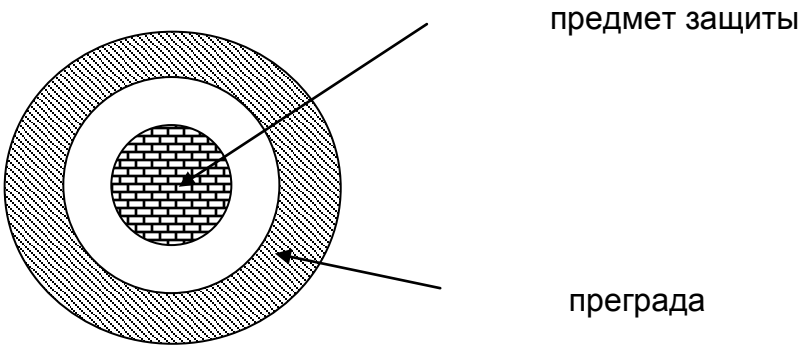

Рис. 3.1. Модель однозвенной защиты

Прочность защиты зависит от свойств преграды. Считается, что прочность созданной преграды достаточна, если стоимость ожидаемых затрат на ее преодоление потенциальным нарушителем превышает стоимость защищаемой информации.

Если обозначить вероятность непреодоления преграды нарушителем через $P_н$, вероятность преодоления преграды нарушителем через $P_п$, то согласно теории вероятности

$$P_н + P_п = 1.$$

В реальном случае у преграды могут быть пути ее обхода. Обозначим вероятность обхода преграды нарушителем через $P_о$. Нарушитель, действующий в одиночку, выберет один из путей: преодоление преграды или обходной вариант. Тогда, учитывая несовместность событий, формальное выражение прочности преграды можно представить в виде

$$P_н = \min \{(1 - P_п) , (1 - P_о)\}.$$

Рассмотрим наиболее опасную ситуацию, когда нарушитель знает и выберет путь с наибольшей вероятностью преодоления преграды. В таком случае можно предположить, что прочность преграды определяется вероятностью ее преодоления или обхода потенциальным нарушителем по пути с наибольшим значением этой вероятности. То есть в случае действий единственного нарушителя прочность защиты определяется ее слабейшим звеном.

У преграды может быть несколько путей обхода. Тогда последнее выражение примет вид

$$P_н = \min \{(1 - P_п), (1 - P_{о1}), (1 - P_{о2}), (1 - P_{о3}), \ldots (1 - - P_{ок})\},$$

где k – количество путей обхода.

Для случая, когда нарушителей более одного и они действуют одновременно (организованная группа) по каждому пути, это выражение с учетом совместности действий будет выглядеть так:

$$P_{н} = (1 - P_{п}) \cdot (1 - P_{о1}) \cdot (1 - P_{о2}) \cdot (1 - P_{о3}) \ldots (1 - P_{ok}).$$

Данная формула применима для неконтролируемой преграды.

Рассмотрим особенности расчета соотношений для контролируемой преграды. Когда к предмету защиты, имеющему постоянную ценность, необходимо и технически возможно обеспечить контроль доступа, обычно применяется постоянно действующая преграда, обладающая свойствами обнаружения и блокировки доступа нарушителя к предмету или объекту защиты.

Для анализа ситуации рассмотрим временную диаграмму процесса контроля и обнаружения НСД, приведенную на рис. 4.2.

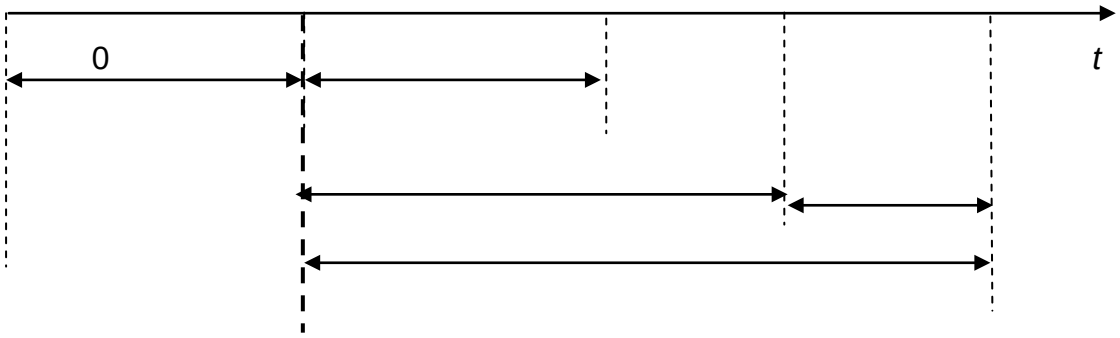

Рис. 3.2. Временная диаграмма процесса контроля и обнаружения НСД:
T – период опроса датчиков; $T_{об}$ – время передачи сигнала и обнаружения НСД;
$T_{б}$ – время блокировки доступа; $T_{нр}$ – время нарушения

Из рис. 4.2 следует, что нарушитель может быть не обнаружен в двух случаях:

а) когда время нарушения меньше периода опроса датчиков: $T_{нр} < T$;

б) когда $T < T_{нр} < T_{об} + T_{б}$.

В случае а) требуется дополнительное условие – попадание интервала времени t в интервал T, т. е. необходима синхронизация действий нарушителя с частотой опроса датчиков обнаружения.

Формально эту задачу можно представить следующим образом. Есть последовательное множество событий в виде контрольных импульсов с расстоянием T между ними и есть определенное множество элементарных событий в виде отрезка длиной $T_{нр}$, который случайным образом накладывается на первое множество. Задача состоит в определении вероятности попадания отрезка $T_{нр}$ на контрольный импульс, если $T_{нр} < T$.

Если обозначить вероятность попадания отрезка на контрольный импульс, то есть вероятность обнаружения нарушения, через P_1, то

$$P_1 = \begin{cases} \frac{T_{нр}}{T}, T_{нр} < T \\ 1, T_{нр} \geq T \end{cases}$$

В случае б), когда $T < T_{нр} < T_{об} + T$, НСД фиксируется наверняка и вероятность обнаружения действий нарушителя будет определяться соотношением между $T_{нр}$ и $(T_{об} + T_б)$.

Величина ожидаемого $T_{нр}$ зависит от многих факторов:

- характера поставленной задачи нарушения,
- метода и способа нарушения,
- технических возможностей и квалификации нарушителя,
- технических возможностей автоматизированной системы.

Поэтому можно говорить о вероятностном характере величины $T_{нр.}$ Если обозначить вероятность обнаружения и блокировки НСД через P_2, то

$$P_2 = \frac{T_{нр}}{T_{об} + T_б}.$$

Для более полного формального представления прочности преграды в виде автоматизированной системы обнаружения и блокировки НСД необходимо учитывать надежность ее функционирования и пути возможного обхода ее нарушителем.

Вероятность отказа системы определяется по формуле

$$P_{отк}(t) = e^{-\lambda t},$$

где λ – интенсивность отказов группы технических средств, составляющих систему обнаружения и блокировки НСД;

t – рассматриваемый интервал времени функционирования системы обнаружения и блокировки НСД.

Исходя из наиболее опасной ситуации, считаем, что отказ системы контроля и НСД могут быть совместными событиями. Поэтому, с учетом этой ситуации формула прочности контролируемой преграды примет вид

$$P_н = \min\{P_2 (1 - P_{отк}), (1 - P_{о1}), (1 - P_{о2}), (1 - P_{о3}), \ldots (1 - P_{ok})\},$$

где $P_о$ и количество путей обхода k определяются экспертным путем на основе анализа принципов построения конкретной системы контроля и блокировки НСД.

В случае, если ценность информации падает с течением времени, за условие достаточности защиты можно принять превышение затрат времени на преодоление преграды нарушителем над временем жизни информации. В качестве такой защиты может быть использовано криптографическое преобразование информации. Возможными путями обхода криптографической преграды могут быть криптоанализ исходного текста зашифрованного сообщения или доступ к действительным значениям ключей шифрования при хранении и передаче.

На практике в большинстве случаев защитный контур (оболочка) состоит из нескольких соединенных между собой преград с различной прочностью (рис. 3.3).

Примером такого вида защиты может служить помещение, в котором хранится аппаратура. В качестве преград с различной прочностью здесь могут служить стены, потолок, пол, окна и замок на двери.

Формальное описание прочности многозвенной оболочки защиты почти полностью совпадает с однозвенной, т. к. наличие нескольких путей обхода одной преграды, не удовлетворяющих заданным требованиям, потребует их перекрытия другими преградами, которые в конечном итоге образуют многозвенную оболочку защиты.

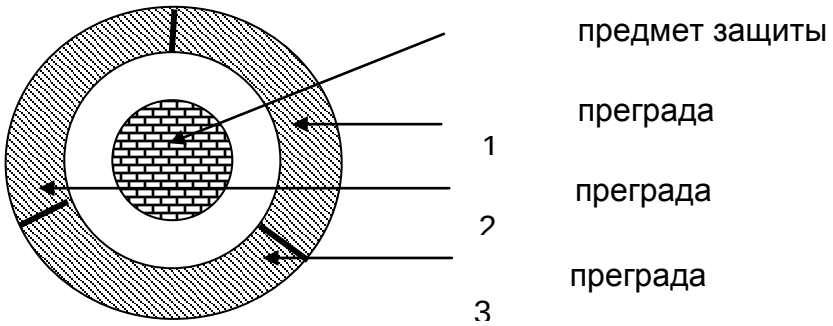

Рис. 3.3. Модель многозвенной защиты

Прочность многозвенной защиты из неконтролируемых преград, построенной для противостояния одному нарушителю, определяется по формуле

$$P_{зи} = \min\{P_{сзи1}, P_{сзи2}, P_{сзиi}, (1 - P_{о1}), (1 - P_{о2}), (1 - P_{о3}), \ldots (1 - P_{оk})\},$$

где $P_{сзиi}$ – прочность i-й преграды;

P_{0k} – вероятность обхода преграды по k-му пути.

Прочность многозвенной защитной оболочки от одного нарушителя равна прочности ее слабейшего звена. Это правило справедливо и для защиты от неорганизованной группы нарушителей, действующих самостоятельно.

Прочность многозвенной защиты, построенной из неконтролируемых преград для защиты от организованной группы квалифицированных нарушителей, рассчитывается следующим образом:

$$P_{зи0} = P_{сзи1} \cdot P_{сзи2} \cdot \ldots P_{сзиi} \cdot (1 - P_{о1}) \cdot (1 - P_{о2}) \cdot (1 - P_{о3}) \ldots (1 - P_{оk}).$$

Прочность многозвенной защиты от организованной группы нарушителей равна произведению вероятностей непреодоления потенциальным нарушителем каждого из звеньев, составляющих эту защиту.

Расчет прочности многозвенной защиты с контролируемыми преградами аналогичен.

Расчеты итоговых прочностей защиты для неконтролируемых и контролируемых преград должны быть раздельными, поскольку исходные данные для них различны и, следовательно, на разные задачи должны быть разные решения – две разные оболочки защиты одного уровня.

Если прочность слабейшего звена защиты удовлетворяет предъявленным требованиям оболочки защиты в целом, возникает вопрос об избыточности прочности на остальных звеньях данной оболочки. Отсюда следует, что экономически целесообразно применять в многозвенной оболочке защиты равнопрочные преграды.

Если звено защиты не удовлетворяет предъявленным требованиям, преграду в этом звене следует заменить на более прочную или данная преграда дублируется еще одной преградой, а иногда двумя и более преградами. Дополнительные преграды должны перекрывать то же количество или более возможных каналов НСД, что и первая.

В этом случае, если обозначить прочность дублирующих друг друга преград соответственно через $P_{д1}$, $P_{д2}$, $P_{д3}$,..$P_{дi}$, то вероятность преодоления каждой из них определяется как вероятность противоположного события: $(1 - P_{д1})$, $(1 - P_{д2})$, $(1 - P_{д3})$, ...$(1 - P_{дi})$.

Считаем, что факты преодоления этих преград нарушителем – события совместные. Это позволяет вероятность преодоления суммарной преграды нарушителем представить в виде

$$P_{п} = (1 - P_{д1}) \cdot (1 - P_{д2}) \cdot (1 - P_{д3}) \ldots (1 - P_{дi}).$$

В ответственных случаях при повышенных требованиях к защите применяется многоуровневая защита, модель которой представлена на рис. 3.4.

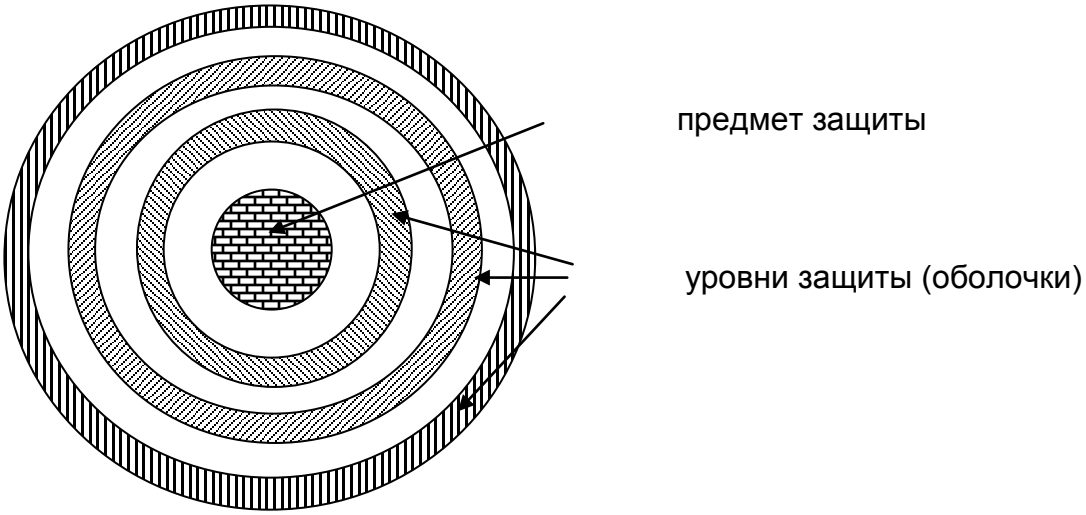

Рис. 3.4. Модель многоуровневой защиты

При расчете суммарной прочности многоуровневой защиты суммируются прочности отдельных уровней.

3.6. Построение систем защиты от угрозы конфиденциальности. Причины и виды утечки информации

Нарушение конфиденциальности происходит в результате утечки информации. Защита информации от утечки – это деятельность, направленная на предотвращение неконтролируемого распространения защищаемой информации в результате ее разглашения, несанкционированного доступа к информации и получения защищаемой информации разведками.

Основными причинами утечки информации являются [3]:

- несоблюдение персоналом норм, требований, правил эксплуатации АС;
- ошибки в проектировании АС и систем защиты АС;
- ведение противостоящей стороной технической и агентурной разведок.

Несоблюдение персоналом норм, требований, правил эксплуатации АС может быть как умышленным, так и непреднамеренным. От ведения противостоящей стороной агентурной разведки этот случай отличает то, что здесь лицом, совершающим несанкционированные действия, двигают личные побудительные мотивы. Причины утечки информации достаточно тесно связаны с видами утечки информации.

В соответствии с ГОСТ Р 50922–96 рассматриваются три вида утечки информации:

- разглашение;
- несанкционированный доступ к информации;

- получение защищаемой информации разведками (как отечественными, так и иностранными).

Под *разглашением* информации понимается несанкционированное доведение защищаемой информации до потребителей, не имеющих права доступа к защищаемой информации.

Согласно [7] *несанкционированный доступ к информации* – доступ к информации, нарушающий установленные правила разграничения доступа, с использованием штатных средств, предоставляемых СВТ или АС. Под НСД понимается получение защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации. При этом заинтересованным субъектом, осуществляющим несанкционированный доступ к информации, может быть государство, юридическое лицо, группа физических лиц, в том числе общественная организация, отдельное физическое лицо.

Получение защищаемой информации разведками может осуществляться с помощью технических средств (техническая разведка) или агентурными методами (агентурная разведка).

3.7. Классификация каналов утечки информации

Канал утечки информации – совокупность источника информации, материального носителя или среды распространения несущего указанную информацию сигнала и средства выделения информации из сигнала или носителя. Одним из основных свойств канала является месторасположение средства выделения информации из сигнала или носителя, которое может быть в пределах контролируемой зоны, охватывающей АС, или вне ее.

При выявлении каналов утечки информации необходимо рассматривать всю совокупность элементов системы, включающую *основное оборудование технических средств обработки информации* (ТСОИ), оконечные устройства, соединительные линии, распределительные и коммутационные устройства, системы электропитания, системы заземления и т. п.

Наряду с основными техническими средствами, непосредственно связанными с обработкой и передачей информации, необходимо учитывать и *вспомогательные технические средства и системы* (ВТСС), такие как технические средства открытой телефонной, факсимильной, громкоговорящей связи, системы охранной и пожарной сигнализации, электрификации, радиофикации, часофикации, электробытовые приборы и др.

В качестве каналов утечки большой интерес представляют вспомогательные средства, выходящие за пределы контролируемой зоны, а также посторонние провода и кабели, к ним не относящиеся, но проходящие через помещения с установленными в них основными и вспомогательными

техническими средствами, металлические трубы систем отопления, водоснабжения и другие токопроводящие металлоконструкции.

Следует помнить о *внутренних* каналах утечки информации, связанных с действиями администрации и обслуживающего персонала, с качеством организации режима работы, тем более что обычно им не придают должного внимания. Из них в первую очередь можно отметить такие каналы утечки, как хищение носителей информации, съем информации с ленты принтера и плохо стертых дискет, использование производственных и технологических отходов, визуальный съем информации с дисплея и принтера, несанкционированное копирование и т. п.

Каналы утечки информации *по физическим принципам* можно разделить на следующие группы [6]:

- акустические (включая и акустопреобразовательные). Связаны с распространением звуковых волн в воздухе или упругих колебаний в других средах;
- электромагнитные (в том числе магнитные и электрические);
- визуально-оптические (наблюдение, фотографирование). В качестве средства выделения информации в данном случае могут рассматриваться фото-, видеокамеры и т. п.;
- материально-вещественные (бумага, фото, магнитные носители, отходы и т. п.);
- информационные. Связаны с доступом к элементам ТКС, носителям информации, самой вводимой и выводимой информации, к программному обеспечению, а также с подключением к линиям связи.

На практике применяется также деление каналов утечки на технические (к ним относятся акустические, визуально-оптические и электромагнитные) и информационные.

3.8. Технические каналы утечки информации

Физические процессы, происходящие в технических средствах при их функционировании, создают в окружающем пространстве излучения, которые в той или иной степени связаны с обрабатываемой информацией (акустическое и электромагнитное излучение, ПЭМИН).

Правомерно предполагать, что образованию каналов утечки информации способствуют также определенные обстоятельства и причины технического характера (несовершенство схемных решений, эксплуатационный износ элементов изделия).

В любых технических средствах существуют те или иные физические преобразователи, которые выполняют соответствующие им функции, основанные на определенном физическом принципе действия. Однако помимо

основных своих функций такие преобразователи в соответствии со своей физической природой способны порождать и дополнительные каналы утечки. Знание всех типов физических преобразователей позволяет решать задачу определения возможных неконтролируемых проявлений физических полей, образующих каналы утечки информации.

Особенности акустических каналов утечки информации

Наиболее ценной акустической информацией чаще всего является речь. Частоты речевых сигналов 16 – 20 000 Гц.

Один и тот же звук разные люди произносят по-разному (своего рода речевой почерк). Звуки речи не одинаково информативны: гласные содержат мало информации о смысле речи, а глухие согласные наиболее информативны.

Мерой силы звукового ощущения является громкость звука. Минимальная громкость соответствует *порогу слышимости*, максимальная – *порогу болевого ощущения*. Оба порога зависят от частоты звука. Человеческому уху свойственно изменение порога слышимости: в условиях тишины слышен писк комара, а в условиях шума трудно услышать громкую речь.

Качество речи оценивается ее *разборчивостью*, представляющей собой статистическую характеристику речи, принимаемой на фоне шумов. Разборчивость — это отношение числа правильно понятых элементов речи (звуков, слогов, слов) к общему числу переданных по каналу элементов. Она может характеризовать качество канала только в среднем значении, допуская флуктуации в ту или иную сторону. Разборчивость речи определяется экспериментально с помощью так называемых артикуляционных испытаний. Объективные измерительные и расчетные оценки разборчивости речи могут производиться с помощью вычисления разборчивости формант. Формантами называются максимумы текущего спектра речи, которые заполняют весь речевой диапазон. Доказано, что восприятие человеком формант обладает свойством аддитивности, т. е. каждый участок речевого диапазона вносит свой вклад в общую разборчивость речи. В акустических измерениях используются октавные или третьоктавные частотные полосы. Для октавного анализа вклады частот русской речи равны следующим значениям:

Частотная полоса, кГц	0,25	0,5	1	2	4	8
Разборчивость формант, %	6,7	12,5	21,2	29,4	25	5,2

От качественного приема (без искажений и помех) каждой частотной полосы зависит суммарная разборчивость. Предельное значение разборчивости формант, при которой возможно понимание смысла речевого сообщения, равно 15 %, что соответствует 25 %-й разборчивости слогов. Задача оценки канала утечки сводится к измерению или вычислению разборчивости речи и сравнению полученного значения с предельным.

Важным является то, какое качество принятого сигнала может обеспечить используемый канал. Для оценки акустического канала при работе с речевой

информацией применяется такая характеристика, как разборчивость речи. Она зависит от следующих факторов:

- ослабления речи в канале;
- реверберации звука;
- уровня вибрационных и акустических шумов в местах установки датчиков;
- чувствительности самих датчиков.

Оперативная оценка этих факторов осложняется тем, что вибрационные и акустические сигналы не поддаются точному расчету. Качество каналов съема оценивают экспериментальным путем с помощью акустических измерений, имитирующих ситуацию контроля информации.

Шумы и помехи, возникающие в месте установки датчика, вызываются многочисленными источниками: автомобильным транспортом, работой механических машин, технических средств в помещениях, разговорами в смежных помещениях и т. п. Характерная особенность шумов — их нестационарность, т. е. изменение уровня времени. Эти изменения зависят от времени суток (вечером уровни шумов намного меньше, чем днем), от дня недели (в выходные дни уровни шумов снижаются), от погодных условий. Маскирующие свойства помех проявляются тем сильнее, чем больше их превышение над полезным сигналом во всей полосе частот речевого диапазона. Наибольшие шумы — уличные, которые создаются автомобильным транспортом, листвой (при наличии ветра), а также дворовые. В здании источниками шумов являются люди (разговоры, шаги), работа механизмов, водопровода, лифта. Средние значения акустических шумов на улице составляют 60...75 дБ и зависят от интенсивности движения автомашин в районе расположения объекта. Разница в уровне шумов от максимального до минимального может составлять до 30 дБ. Следует иметь в виду, что существующая норма допустимого уровня акустических шумов в рабочих помещениях равна 50 дБ. Этот уровень можно брать в качестве расчетного, если неизвестны конкретные показатели шумности в смежных посторонних помещениях. Все приведенные значения шумов даны для широкополосных источников помех.

Акустические колебания в помещении складываются из шумов источников, находящихся внутри помещения, и шумов источников вне помещения.

Основные пути прохождения акустических волн из помещения:

- воздушный перенос: прохождение через открытые окна, двери, щели, поры, вентиляционные воздуховоды;
- материальный перенос: прохождение через материал стены или по трубам отопления, газопровода, водопровода в виде продольных колебаний;

- мембранный перенос: передача колебаний посредством поперечных колебаний перегородки (стекла, стены и пр.).

При рассмотрении первого пути говорят об акустическом канале утечки, второй и третий образуют вибрационный канал.

В воздушных каналах утечки информации средой распространения акустических сигналов является воздух, и для их перехвата используются миниатюрные высокочувствительные и направленные микрофоны, которые соединяются с диктофонами или специальными минипередатчиками. Подобные автономные устройства, объединяющие микрофоны и передатчики, обычно называют закладными устройствами или акустическими закладками. Перехваченная этими устройствами акустическая информация может передаваться по радиоканалу, по сети переменного тока, соединительным линиям, посторонним проводникам, трубам и т. п. В этом случае прием осуществляется, как правило, на специальные приемные устройства. Особого внимания заслуживают закладные устройства, прием информации с которых можно осуществить с телефонного аппарата.

Необходимо отметить, что акустический канал может быть источником утечки не только речевой информации. В литературе описаны случаи, когда с помощью статистической обработки акустической информации с принтера или клавиатуры удавалось перехватывать компьютерную текстовую информацию, в том числе осуществлять съем информации по системе централизованной вентиляции.

В вибрационных, или структурных, каналах утечки информации средой распространения акустических сигналов является не воздух, а конструкции зданий (стены, потолки, полы), трубы водо- и теплоснабжения, канализации и другие твердые тела. В этом случае для перехвата акустических сигналов используются контактные, электронные (с усилителем) и радиостетоскопы (при передаче по радиоканалу).

При облучении лазерным лучом вибрирующих в акустическом поле тонких отражающих поверхностей, таких как стекла окон, зеркал, картин и т. п., создается оптико-электронный, или лазерный, канал утечки акустической информации. Отраженное лазерное излучение модулируется по амплитуде и фазе и принимается приемником оптического излучения, при демодуляции которого выделяется речевая информация. Для перехвата речевой информации по данному каналу используются локационные системы, работающие обычно в ближнем инфракрасном диапазоне волн и известные как «лазерные микрофоны». Дальность перехвата составляет несколько сотен метров.

Меры по защите объекта, как правило, направлены на перекрытие возможных каналов съема с помощью инженерных средств, проведение работ по звукоизоляции (для уменьшения воздушного и материального переноса звука через перегородки следует делать их слоистыми, подбирая материалы с резко отличающимися акустическими сопротивлениями, для уменьшения мембранного переноса стены делают массивными и т. д.) и зашумлению строительных конструкций защищаемого здания с помощью специального

генератора помех. При проектировании такой системы крайне важна точная оценка объекта, так как виброакустическими методами съема информации пользуются квалифицированные профессионалы с применением самой высококачественной техники.

Преобразователи аудиоинформации

Преобразователем является прибор, который преобразует изменения одной физической величины в изменения другой.

Акустическая энергия, возникающая при разговоре, может вызвать акустические (т. е. механические) колебания элементов электронной аппаратуры, что в свою очередь приводит к появлению или изменению электромагнитного излучения.

Любой преобразователь характеризуется определенными параметрами. Наиболее важными из них являются:

- чувствительность – отношение изменения выходного сигнала к изменению сигнала на его входе;
- разрешающая способность – наибольшая точность, с которой осуществляется преобразование;
- линейность – равномерность изменения выходного сигнала в зависимости от входного;
- инертность (время отклика) – время установления выходного сигнала в ответ на изменение входного сигнала;
- рабочая полоса частот – частотный диапазон, в пределах которого воздействие на входе преобразователя создает на выходе допустимый уровень сигнала.

По физической природе имеется значительное количество различных первичных преобразователей, среди которых выделяются следующие группы:

- индуктивные;
- емкостные;
- пьезоэлектрические;
- оптические преобразователи.

Наиболее чувствительными к акустическим воздействиям элементами радиоэлектронной аппаратуры являются катушки индуктивности и конденсаторы переменной емкости.

1. *Индуктивные преобразователи. Микрофонный эффект*.

Рассмотрим акустическое воздействие на катушку индуктивности с сердечником. Механизм и условия возникновения ЭДС индукции в такой катушке сводятся к следующему. Под воздействием акустического давления появляется вибрация корпуса и обмотки катушки. Вибрация вызывает колебания проводов обмотки в магнитном поле, что и приводит к появлению

ЭДС индукции на концах катушки. Она зависит от вектора магнитной индукции, магнитной проницаемости сердечника, угла между вектором и осью катушки, угла между вектором и осью сердечника и площадей поперечных сечений сердечника и катушки. Данный эффект непосредственно используется в электродинамических микрофонах, поэтому получил название микрофонного эффекта.

Индуктивные преобразователи подразделяются на электромагнитные, электродинамические и магнитострикционные.

К электромагнитным преобразователям относятся такие устройства как громкоговорители, электрические звонки (в том числе и вызывные звонки телефонных аппаратов), электрорадиоизмерительные приборы.

Типичный образец индуктивного акустоэлектрического преобразователя – электромеханический вызывной звонок телефонного аппарата, микрофонный эффект которого проявляется при положенной телефонной трубке. По тому же принципу образуется микрофонный эффект и в отдельных типах электромеханических реле различного назначения. Акустические колебания воздействуют на якорь реле. Колебания якоря изменяют магнитный поток реле, замыкающийся по воздуху, что приводит к появлению на выходе катушки реле ЭДС микрофонного эффекта.

Динамические головки прямого излучения, устанавливаемые в абонентских громкоговорителях, имеют достаточно высокую чувствительность к акустическому воздействию и довольно равномерную в речевом диапазоне частот амплитудно-частотную характеристику, что обеспечивает высокую разборчивость речевых сигналов.

В магнитоэлектрическом измерительном приборе имеются подвижный постоянный магнит и подвижная рамка, которая поворачивается вокруг своей оси под воздействием собственного магнитного поля, создаваемого измеряемым напряжением, и магнитного поля постоянного магнита. Рамка соединена со стрелкой, конец которой перемещается по шкале измерения. Если акустические колебания воздействуют на рамку, она вращается под их давлением и на ее концах возникает ЭДС индукции.

Практически аналогичная ситуация будет при воздействии акустических колебаний на электромагнитный измерительный прибор. Различие между магнитоэлектрическим и электромагнитным приборами сводится к тому, что в электромагнитном приборе вместо постоянного магнита используется электромагнит.

Следует отметить, что ЭДС микрофонного эффекта возникает и может использоваться в состоянии покоя прибора, когда он не применяется для конкретных измерений.

Примерами индукционных акустоэлектрических преобразователей являются различные трансформаторы (повышающие, понижающие, входные, выходные, питания и др.).

Трансформатор состоит из двух (или более) изолированных друг от друга катушек (обмоток) с разными числами витков и замкнутого сердечника из мягкой стали или феррита.

Акустическое влияние на сердечник и обмотку трансформатора (например, на входной трансформатор усилителя звуковых частот) приведет к появлению микрофонного эффекта. Если ЭДС индукции появляется в первичной обмотке, то во вторичной обмотке она увеличивается в коэффициент трансформации раз.

Магнитострикция — изменение размеров и формы кристаллического тела при намагничивании — вызывается изменением энергетического состояния кристаллической решетки в магнитном поле и, как следствие, расстояний между узлами решетки. Наибольших значений магнитострикция достигает в ферро- и ферритомагнетиках, в которых магнитное взаимодействие частиц особенно велико.

Обратное по отношению к магнитострикции явление — Виллари-эффект, т. е. изменение намагничиваемости тела при его деформации. Виллари-эффект обусловлен изменением под действием механических напряжений доменной структуры ферромагнетика, определяющей его намагниченность. В усилителях с очень большим коэффициентом усиления входной трансформатор на ферритах способен преобразовывать механические колебания в электрические.

2. *Емкостные преобразователи*.

Емкостные преобразовывающие элементы превращают изменение емкости в изменение электрического потенциала, тока, напряжения.

Емкость конденсатора зависит от расстояния между пластинами. Воздействующее на пластины акустическое давление, изменяя расстояние между пластинами, приводит к изменению емкости.

Конденсаторы переменной емкости с воздушным диэлектриком являются одним из основных элементов перестраиваемых колебательных контуров генераторных систем. Они устроены так, что система пластин вдвигается в другую систему пластин, образуя конденсатор переменной емкости. Изменяющееся акустическое давление, воздействуя на такой конденсатор, изменяет его емкость, а следовательно, и характеристики устройства, в котором он установлен.

3. *Пьезоэлектрический преобразователь*.

Изучение свойств твердых диэлектриков показало, что некоторые из них поляризуются не только с помощью электрического поля, но и в процессе деформации при механических воздействиях на них. Поляризация диэлектрика при механическом воздействии называется прямым пьезоэлектрическим эффектом. Этот эффект имеется у кристаллов кварца и у всех сегнетоэлектриков. У пьезокристаллов наблюдается и обратное явление. Если пластину, вырезанную из пьезокристалла, поместить в электрическое поле,

зарядив металлические обкладки, то она поляризуется и деформируется, например сжимается. При перемене направления внешнего электрического поля сжатие пластинки сменяется ее растяжением (расширением). Такое явление называется обратным пьезоэлектрическим эффектом.

Кварцевые пластины широко используются в пьезоэлектрических микрофонах, охранных датчиках, стабилизаторах, генераторах электрического микрофона.

4. *Оптические преобразователи*.

К оптическим преобразователям относятся приборы, преобразующие световую энергию в электрическую и обратно.

Что касается технических каналов утечки информации, то в оптических системах опасным является акустооптический эффект. Акустооптический эффект — это явление преломления, отражения или рассеяния света, вызванное упругими деформациями стеклянных отражающих поверхностей или волоконно-оптических кабелей под воздействием звуковых колебаний. Волоконные световоды как преобразователи механического давления в изменение интенсивности света являются источником утечки акустической информации за счет акустооптического (или акустоэлектрического) преобразования — микрофонного эффекта в волоконно-оптических системах передачи информации (используется также в охранных системах).

Основным элементом оптического кабеля волоконно-оптических систем является волоконный световод в виде тонкого стеклянного волокна цилиндрической формы. Волоконный световод имеет двухслойную конструкцию и состоит из сердцевины и оболочки с различными оптическими характеристиками (показателями преломления). Сердцевина служит для передачи электромагнитной энергии. Назначение оболочки — создание лучших условий отражения на границе сердцевина–оболочка и защита от излучения в окружающее пространство.

Передача волны по световоду осуществляется за счет отражений ее от границы сердечника и оболочки, имеющих разные показатели преломления. В современных волоконно-оптических системах в процессе передачи информации используется модуляция источника света по амплитуде, интенсивности и поляризации.

Внешнее акустическое воздействие на волоконно-оптический кабель приводит к изменению его геометрических размеров (толщины), что вызывает изменение пути движения света, т. е. приводит к изменению интенсивности, причем пропорционально значению этого давления.

При слабом закреплении волокон в разъемном соединителе световодов проявляется акустический эффект модуляции света акустическими полями. Акустические волны вызывают смещение соединяемых концов световода относительно друг друга. Таким образом осуществляется амплитудная модуляция излучения, проходящего по волокну.

В контролируемой зоне следует свести к минимуму количество имеющихся преобразователей. Меры защиты от утечки информации через аудиопреобразователи те же, что и меры защиты от утечки через электромагнитные каналы.

Электромагнитные каналы утечки

Каждое электрическое (электронное) устройство является источником магнитных и электромагнитных полей широкого спектра, характер которых определяется назначением и схемными решениями, мощностью устройства, материалами, из которых оно изготовлено, и его конструкцией.

Вокруг проводника, по которому протекает ток *I,* вызванный напряжением *U*, создается магнитное поле с напряженностью *H* и электрическое поле с напряженностью *E* (рис. 3.9).

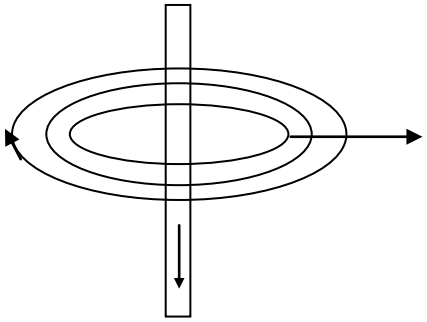

Рис. 3.9. Распределение магнитного и электрического поля вокруг проводника с током

Изменение во времени тока приводит к изменению во времени электрического и магнитного полей. Вызванные изменением тока в проводнике изменяющиеся во времени электрическое и магнитное поля представляют собой единое изменяющееся электромагнитное поле, распространяющееся в пространстве, свойства которого целиком и полностью описываются уравнениями Максвелла.

Известно, что характер поля изменяется в зависимости от расстояния до передающего устройства. Поле делится на две зоны: ближнюю и дальнюю.

В дальней зоне (начиная от расстояний, больших 6λ от источника возмущения) электрическое поле принимает плоскую конфигурацию и распространяется в виде плоской волны, энергия которой делится поровну между электрической и магнитной компонентами. Дальняя зона — это область пространства, в которой распространение от источника существенно превышает длину волны. Граница между дальней и ближней зонами находится на расстоянии около 0,5 м от источника излучения для частоты 100 МГц и 50 м для частоты 1 МГц.

В ближней зоне преобладает магнитная либо электрическая составляющая поля. Сильные магнитные поля, как правило, создаются цепями

с низким волновым сопротивлением, большим током и малым перепадом напряжений.

Для поля с преобладающей электрической компонентой волновое сопротивление существенно больше, а для преобладающего магнитного поля — существенно меньше значения волнового сопротивления для плоской волны (Z = 377 Ом).

Изменение тока во времени может носить импульсный характер или подчиняться любому другому закону. Каждый такой процесс на основе известного из математики преобразования Фурье может быть представлен в виде суммы гармонических колебаний с различными амплитудами для каждой частоты, причем частоты изменяются в пределах от нуля до бесконечности. Зависимость амплитуд этих гармонических составляющих от частоты – это спектр сигнала (в рассматриваемом случае – электромагнитного излучения). Спектр характеризует распределение энергии в поле излучения. В зависимости от того, на каких частотах устройство излучает наиболее интенсивно, излучатели электромагнитных сигналов подразделяют на низкочастотные, высокочастотные и оптические.

Низкочастотными излучателями электромагнитных колебаний в основном являются звукоусилительные устройства различного функционального назначения и конструктивного исполнения. В ближней зоне этих устройств наиболее мощным выступает магнитное поле информативного сигнала. Такое поле усилительных систем достаточно просто обнаруживается и принимается посредством магнитной антенны и селективного усилителя звуковых частот.

К группе высокочастотных излучателей относятся ВЧ-автогенераторы, модуляторы ВЧ-колебаний и устройства, генерирующие паразитные высокочастотные колебания по различным причинам и в различных условиях.

Источниками сигнала выступают ВЧ-генераторы радиоприемников, телевизоров, измерительных генераторов, мониторы ЭВМ, модуляторы ВЧ-колебаний. Довольно опасным источником высокочастотных колебаний могут быть усилители и другие активные элементы технических средств в режиме паразитной генерации за счет нежелательной положительной обратной связи.

В качестве высокочастотного излучателя рассматривается любое устройство, содержащее элементы с нелинейными характеристиками (диоды, транзисторы, микросхемы), порождающими нежелательные составляющие высокочастотного характера.

Спектр излучения обычно не поддается аналитическому расчету, т. к. его форма зависит от многих факторов; прежде всего это следующие:

- рабочие частоты устройства, их гармоники и комбинационные частоты;
- расположение и длина проводников;
- расположение и конструкция реактивных элементов (конденсаторов и индуктивных катушек);

- тип корпуса, наличие в нем щелей, отверстий и т. п.

При анализе спектра следует разделять информативное ПЭМИ и неинформативное ПЭМИ, а также реальные возможности восстановления информации из принятого ПЭМИ.

Наиболее опасными являются следующие виды излучений и наводок:

- электромагнитные излучения элементов ТСОИ (носителем информации является электрический ток, напряжение, частота или фаза которого изменяются по закону информационного сигнала);
- электромагнитные излучения на частотах работы высокочастотных генераторов ТСОИ и ВТСС (в результате внешних воздействий информационного сигнала на элементах генераторов наводятся электрические сигналы, которые могут вызвать непреднамеренную модуляцию собственных высокочастотных колебаний генераторов и излучение в окружающее пространство [14]);
- электромагнитные излучения на частотах самовозбуждения усилителей низкой частоты ТСПИ (самовозбуждение возможно за счет случайных преобразований отрицательных обратных связей в паразитные положительные, что приводит к переводу усилителя из режима усиления в режим автогенерации сигналов, причем сигнал на частотах самовозбуждения, как правило, оказывается промодулированным информационным сигналом);
- наводки электромагнитных излучений ТСОИ (возникают при излучении элементами ТСОИ информационных сигналов, а также при наличии гальванической связи соединительных линий ТСОИ и посторонних проводников или линий ВТСС);
- просачивание информационных сигналов в цепи электропитания (возможно при наличии магнитной связи между выходным трансформатором усилителя и трансформатором электропитания, а также за счет неравномерной нагрузки на выпрямитель, что приводит к изменению потребляемого тока по закону изменения информационного сигнала);
- просачивание информационных сигналов в цепи заземления (образуется за счет гальванической связи с землей различных проводников, выходящих за пределы контролируемой зоны, в том числе нулевого провода сети электропитания, экранов, металлических труб систем отопления и водоснабжения, металлической арматуры и т. п.);
- съем информации с использованием закладных устройств, представляющих собой миниатюрные передатчики, устанавливаемые в ТСОИ, излучения которых модулируются информационным сигналом и принимаются за пределами контролируемой зоны.

Параметрический канал утечки информации формируется путем «высокочастотного облучения» ТСОИ, при взаимодействии электромагнитного поля которого с элементами ТСОИ происходит переизлучение электромагнитного поля, промодулированного информационным сигналом.

Взаимные влияния сигналов проявляются в линиях связи (табл. 5.1). Существуют реальные условия наводок с одного провода на другой, параллельный ему провод любой длины. В соответствии с явлением взаимной индукции ЭДС индукции наводится во всех проводниках, находящихся вблизи других проводников, ток в которых изменяется с течением времени, при этом ЭДС взаимной индукции пропорциональна скорости изменения тока.

Таблица 5.1

Влияния в цепях связи и стандартные меры защиты

Тип линии	Преобладающее влияние	Меры защиты
Воздушные линии связи	Систематическое влияние[1], возрастающее с увеличением частоты сигнала	Скрещивание цепей, оптимальное расположение цепей
Коаксиальный кабель	Систематическое влияние через третьи цепи (с повышением частоты влияние убывает вследствие поверхностного эффекта)	Экранирование и ограничение диапазона рабочих частот снизу
Симметричный кабель	Систематическое и случайное[2] влияния, возрастающие с частотой	Оптимизация шагов скрутки и конструкций кабеля, пространственное разделение цепей, экранирование
Оптический кабель	Систематическое и случайное влияния (от частоты не зависят)	Экранирование оптических волокон, пространственное разделение отдельных волокон

[1] Систематическое влияние – взаимные наводки, возникающие по всей длины линии

[2] Случайное влияние – влияние, возникающее вследствие случайных причин и не поддающееся точной оценке.

Особое внимание следует обратить на перехват информации при ее передаче по каналам связи. Это вызвано тем, что в данном случае обеспечивается свободный несанкционированный доступ к передаваемым сигналам, особенно в случае использования радиоканала. В зависимости от вида канала связи технические каналы перехвата информации можно разделить на электромагнитные, электрические и индукционные.

Электромагнитные излучения передатчиков средств связи, модулированные информационным сигналом, могут перехватываться естественным образом с использованием стандартных технических средств. Электромагнитный канал перехвата информации широко применяется для прослушивания телефонных разговоров, ведущихся по радиотелефонам, сотовым телефонам или по радиорелейным и спутниковым линиям связи.

Электрический канал перехвата информации, передаваемой по кабельным линиям связи, предполагает контактное подключение к этим линиям. Электрический канал наиболее часто используется для перехвата телефонных разговоров, при этом перехватываемая информация может быть записана на диктофон или передана по радиоканалу. Подобные устройства, подключаемые к телефонным линиям связи и содержащие радиопередатчики для ретрансляции перехваченной информации, обычно называются телефонными закладками.

Однако непосредственное электрическое подключение аппаратуры перехвата является компрометирующим признаком. Поэтому чаще используется индукционный канал перехвата, не требующий контактного подключения к каналам связи. Современные индукционные датчики, по сообщениям открытой печати, способны снимать информацию с кабелей, защищенных не только изоляцией, но и двойной броней из стальной ленты и стальной проволоки, которые плотно обвивают кабель. Единственным гарантированным методом защиты информации в этом случае является криптографическая защита.

Для перекрытия электромагнитных каналов утечки информации используются пассивные и активные методы. К пассивным относятся экранирование элементов аппаратуры, устройств и линий связи, фильтрация сигналов в цепях питания и заземления. Активный метод – радиотехническое зашумление, используемое для закрытия (маскировки) побочных электромагнитных излучений и наводок. При этом спектр и энергия шумового сигнала подбираются таким образом, чтобы гарантировать невозможность выделения информативного сигнала.

Визуально-оптические каналы утечки

В последнее время стало уделяться большое внимание утечке визуальной информации, получаемой в виде изображений объектов или копий документов путем наблюдения за объектом, съемки объекта и съемки (копирования) документов. В зависимости от условий наблюдения обычно используются

соответствующие технические средства, в том числе: оптика (бинокли, подзорные трубы, телескопы, монокуляры), телекамеры, приборы ночного видения, тепловизоры и т. п.

Для документирования результатов наблюдения проводится съемка объектов с помощью фотографических и телевизионных средств, соответствующих условиям съемки. Для снятия копий документов используются электронные и специальные (закамуфлированные) фотоаппараты. Для дистанционного съема видовой информации используют видеозакладки.

3.9. Информационные каналы утечки информации

Информационный канал может быть разделен на следующие каналы:

- канал коммутируемых линий связи;
- канал выделенных линий связи;
- канал локальной сети;
- канал машинных носителей информации;
- канал терминальных и периферийных устройств.

Утечка информации из канала связи при использовании специальных технических средств съема информации была рассмотрена выше.

В последнее время наиболее динамично развиваются методы съема компьютерной информации. В этом направлении используются:

- аппаратные закладки;
- вредоносные программы.

Основные возможности несанкционированного доступа связаны с использованием специального математического обеспечения, включающего в себя такие составляющие, как компьютерные вирусы, «логические бомбы», «троянские кони», программные закладки и т. п. [6].

Вредоносная программа (ВП) – программа, предназначенная для несанкционированного копирования, модификации, блокирования, уничтожения компьютерной информации.

Часто ВП доставляется к месту постоянного размещения через привлекательную для пользователя программу («троянскую» программу). То есть для «троянской» программы характерно наличие встроенной структуры или функции, скрытно выполняющей вредоносные действия. При запуске или на этапе инсталяции параллельно идут два процесса: документированный и недокументированный.

ВП можно разделить на две большие категории:

1) вирусы. Основные свойства вирусов: паразитическое существование, размещение внутри программного файла или в другом месте, способность к саморазмножению – копированию, выраженные деструктивные функции. Основная угроза со стороны вирусов – угроза целостности;

2) программные закладки. Основные свойства: скрытность работы на всех этапах жизненного цикла, явно выраженные «шпионские» функции, частое отсутствие механизма саморазмножения, хотя возможно наличие механизма самоликвидации.

В настоящее время известно большое количество программных закладок, основные функции которых следующие:

- слежение за пользователем;
- раскрытие паролей, ключей;
- изучение обрабатываемой информации.

Вредоносные программы могут быть внедрены в прикладные программы, утилиты и сервисные программы, подсистему безопасности, реестр, ядро, командный интерпретатор, BIOS, драйверы устройств, аппаратные средства. ВП, внедренные на уровень ядра и ниже, невидимы для пользователя.

Для защиты от воздействия ВП и адекватного оценивания возможности и последствий заражения АС пользователь должен иметь представление о механизме действия ВП. В целях безопасной работы необходимо соблюдать ряд правил, которые апробированы на практике и показали свою высокую эффективность:

1) использовать программные продукты, полученные законным официальным путем. Вероятность наличия ВП в «пиратской» копии во много раз выше, чем в официально полученном программном обеспечении;
2) дублировать информацию;
3) регулярно использовать антивирусные средства;
4) особую осторожность следует проявлять при использовании новых съемных носителей информации и новых файлов. Новые дискеты обязательно должны быть проверены на отсутствие загрузочных и файловых вирусов, а полученные файлы – на наличие файловых вирусов;
5) при работе в распределенных системах или в системах коллективного пользования целесообразно новые сменные носители информации и вводимые в систему файлы проверять на специально выделенной для этой цели ЭВМ;
6) если не предполагается осуществлять запись информации на носитель, то необходимо заблокировать выполнение этой операции.

Неукоснительное следование приведенным рекомендациям позволяет значительно уменьшить вероятность проникновения ВП в систему и защищает пользователя от потерь информации.

В настоящее время межсетевые экраны являются достаточно эффективным средством защиты корпоративных сетей и их сегментов от внешних угроз, а также от несанкционированных взаимодействий локальных пользователей с внешними системами. Они обеспечивают высокоуровневую

поддержку политики безопасности организации по отношению ко всем протоколам семейства TCP/IP. Кроме того, современные межсетевые экраны характеризуются прозрачностью для легальных пользователей, большим быстродействием и высокой эффективностью. Основной тенденцией развития средств сетевой защиты является интеграция, в частности интеграция межсетевых экранов с криптографическими и антивирусными средствами, а также средствами анализа уровня обеспечения безопасности.

Однако не следует забывать, что, несмотря на присущие межсетевым экранам достоинства, в настоящее время они не решают всего комплекса задач по обеспечению безопасности в открытых сетях.

Заключение

Утечка информации по техническим и информационным каналам представляет реальную угрозу безопасности информации.

При оценке степени опасности технических каналов утечки следует иметь в виду, что не всегда наличие носителя (акустического или электромагнитного поля) является фактором, достаточным для съема информации. Например, при низкой разборчивости речи невозможно восстановить ее смысл. Побочные электромагнитные излучения электронной аппаратуры могут не нести информативного сигнала (например, излучение, возникшее вследствие генерации тактовых импульсов СВТ). Для объективной оценки проводят специальные исследования оборудования и специальные проверки рабочих помещений. Такого рода исследования и проверки выполняются организациями, имеющими лицензии на соответствующий вид деятельности. При выявлении технических каналов утечки информации применяются меры по их перекрытию.

При решении задач, связанных с обеспечением информационной безопасности, необходимо использовать комплексный подход, включающий в себя применение не только технических средств, но и правовых методов, а также организационные меры защиты информации.

Заключение

Защищать ТКС необходимо от всех видов случайных и преднамеренных воздействий: стихийных бедствий и аварий, сбоев и отказов технических средств, ошибок персонала и пользователей, ошибок в программах и от преднамеренных действий злоумышленников.

Имеется широчайший спектр вариантов путей и методов несанкционированного доступа к данным и вмешательства в процессы обработки и обмена информацией. Анализ всех уязвимостей системы, оценка возможного ущерба позволят верно определить мероприятия по защите информации. Расчет эффективности защитных мероприятий можно

производить различными методами в зависимости от свойств защищаемой информации и модели нарушителя.

Правильно построенная (адекватная реальности) модель нарушителя, в которой отражаются его практические и теоретические возможности, априорные знания, время и место действия и другие характеристики, – важная составляющая успешного проведения анализа риска и определения требований к составу и характеристикам системы защиты.

Утечка информации по техническим и информационным каналам представляет реальную угрозу безопасности информации.

При оценке степени опасности технических каналов утечки следует иметь в виду, что не всегда наличие носителя (акустического или электромагнитного поля) является фактором, достаточным для съема информации. Например, при низкой разборчивости речи невозможно восстановить ее смысл. Побочные электромагнитные излучения электронной аппаратуры могут не нести информативного сигнала (например, излучение, возникшее вследствие генерации тактовых импульсов СВТ). Для объективной оценки проводят специальные исследования оборудования и специальные проверки рабочих помещений. Такого рода исследования и проверки выполняются организациями, имеющими лицензии на соответствующий вид деятельности. При выявлении технических каналов утечки информации применяются меры по их перекрытию.

При решении задач, связанных с обеспечением информационной безопасности, необходимо использовать комплексный подход, включающий в себя применение не только технических средств, но и правовых методов, а также организационные меры защиты информации.