**Лекции 2 Угрозы информационной безопасности. Построение систем защиты от угрозы нарушения конфиденциальности**

1. Анализ уязвимостей системы. Классификация угроз информационной безопасности.
2. Основные направления и методы реализации угроз. Неформальная модель нарушителя.
3. Оценка уязвимости системы.
4. Определение и основные способы несанкционированного доступа. Методы защиты от НСД. Организационные методы защиты от НСД.
5. Инженерно-технические методы защиты от НСД. Построение систем защиты от угрозы утечки по техническим каналам. Идентификация и аутентификация.
6. Основные направления и цели использования криптографических методов. Защита от угрозы нарушения конфиденциальности на уровне содержания информации.

## 1 Анализ уязвимостей системы. Классификация угроз информационной безопасности

*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 информационной системы, 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. Анализ уязвимостей — обязательная процедура при аттестации объекта информатизации. В связи с возможностью появления новых уязвимостей необходим их периодический анализ на уже аттестованном объекте.

*Классификация угроз информационной безопасности*

*Угроза* — это фактор, стремящийся нарушить работу системы.

В настоящее время рассматривается достаточно обширный перечень угроз информационной безопасности, 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 требований к системе защиты. При этом угрозы, соответствующие каждому признаку классификации, позволяют уточнить требования.

Для защищаемой системы составляют не полный перечень угроз, а перечень классов угроз, определяемых по ряду базовых признаков. Это связано с тем, что описать полное

множество угроз невозможно из-за большого количества факторов, влияющих на информацию.

Например, можно предложить классифицировать угрозы по следующим признакам:

1. Природа возникновения: естественные угрозы (связанные с природными процессами) и искусственные (вызванные деятельностью человека).

2. Степень преднамеренности проявления: случайные или преднамеренные.

3. Источник угроз: природная среда, человек, санкционированные программно-аппаратные средства, несанкционированные программно-аппаратные средства.

4. Положение источника угроз: в пределах или вне контролируемой зоны.

5. Зависимость от активности системы: проявляются только в процессе обработки данных или в любое время.

6. Степень воздействия на систему: пассивные, активные (вносят изменения в структуру и содержание системы).

7. Этап доступа к ресурсам: на этапе доступа, после получения доступа.

8. Способ доступа к ресурсам: стандартный, нестандартный.

9. Место расположения информации: внешние носители, оперативная помять, линии связи, устройства ввода-вывода.

Вне зависимости от конкретных видов угроз было признано целесообразным связать угрозы с основными свойствами защищаемой информации.

Соответственно для информационных 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 информационной 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 информационной 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 постоянным — запрашиваемый ресурс никогда не будет получен, или может вызывать только задержку запрашиваемого ресурса.

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 1960-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, атакующая сторона должна преодолеть эту систему. Поскольку преодоление защиты также представляет собой угрозу, для защищенных систем будем рассматривать ее четвертый вид — *угрозу раскрытия параметров системы, 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 системы 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 отличия защищенных информационных систем от открытых. Для последних угроза разведки параметров системы считается реализованной.

## 2 Основные направления и методы реализации угроз. Неформальная модель нарушителя

*Основные направления и методы реализации угроз*

К основным направлениям реализации злоумышленником информационных угроз относятся:

· 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 программных или технических механизмов, нарушающих предполагаемую структуру и функции системы.

К числу основных методов реализации угроз информационной безопасности относятся:

· 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 системой;

· получение злоумышленником данных о применяемых системах защиты;

· определение способа представления информации;

· определение злоумышленником содержания данных, обрабатываемых в системе, на качественном уровне (применяется для мониторинга 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 системы 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 носителей информации;

· внесение пользователем несанкционированных изменений в программно-аппаратные компоненты системы 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 носителей информации без уничтожения;

· проявление ошибок проектирования и разработки аппаратных и программных компонентов;

· искажение соответствия синтаксических и семантических конструкций языка;

· запрет на использование информации.

Перечисленные методы реализации угроз охватывают все уровни представления информации.

*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 системы.

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 системе 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: · руководители различных уровней должностной иерархии.

· пользователи системы;

· сотрудники отделов разработки и сопровождения программного обеспечения;

· персонал, обслуживающий технические средства;

· технический персонал, обслуживающий здания (уборщики, электрики, сантехники и др.);

· сотрудники службы безопасности.

*Посторонние лица,* которые могут быть нарушителями:

· посетители;

· клиенты;

· 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);

· 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.

Классификация нарушителей

*По уровню знаний о системе*:

1) знание функциональных особенностей, основных закономерностей формирования в системе массивов данных и потоков запросов к ним, умение пользоваться штатными средствами;

2) обладание высоким уровнем знаний и опытом работы с техническими средствами системы, а также опытом их обслуживания;

3) обладание высоким уровнем знаний в области программирования и вычислительной техники, проектирования и эксплуатации автоматизированных информационных систем;

4) знание структуры, функций и механизмов действия средств защиты, их сильные и слабые стороны.

*По уровню возможностей*:

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

Второй уровень определяет возможность создания и запуска собственных программ с новыми функциями по обработке информации.

Третий уровень определяет возможность управления функционированием системы, т. е. воздействием на базовое программное обеспечение системы и на состав и конфигурацию ее оборудования.

Четвертый уровень определяет весь объем возможностей лиц, осуществляющих проектирование, реализацию и ремонт технических средств системы, вплоть до включения в состав 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 информационной системе, 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 автоматизированной системе».

*По времени действия*:

· в процессе функционирования (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, 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;

· с рабочих мест конечных пользователей (операторов);
· с доступом в зону данных (баз данных, архивов и т. п.);
· с доступом в зону управления средствами обеспечения безопасности.

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 Оценка уязвимости системы

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

Ряд специалистов в области информационной безопасности разделяют методы и средства защиты от случайных и от преднамеренных угроз [6].

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 информационной системе. В соответствии с характером и важностью этих данных выбираются ожидаемая квалификация и модель поведения потенциального нарушителя.

Рассмотрим ситуацию, когда 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. Например, вход в систему со стороны клавиатуры 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 [6].

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 несанкционированного доступа) и размещаемых на каналах доступа 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 информационной 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 несанкционированного доступа заключается в применении на возможных каналах доступа к информации средств контроля, блокировки и предупреждения событий. Средства контроля и блокировки устанавливаются на возможных каналах доступа, 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.

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

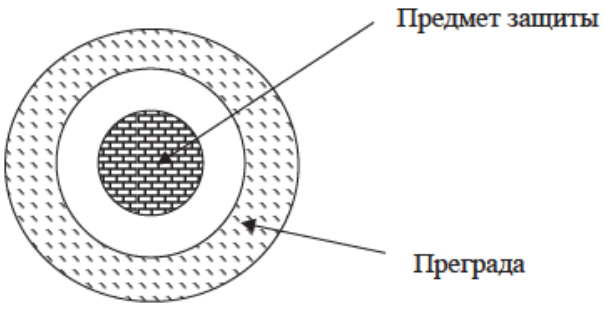


Рис. 3.1 - Модель однозвенной защиты

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

$$P_н = \min \{(1 — P_п), (1 — P_{о1})\}.$$

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

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

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:

$$P_н = (1 — P_п)\,(1 — P_{о1})\,(1 — P_{о2})\,(1 — P_{о3}),\ \ldots\ (1 — P_{оk}).$$

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 несанкционированного доступа, приведенную на рис. 3.2.

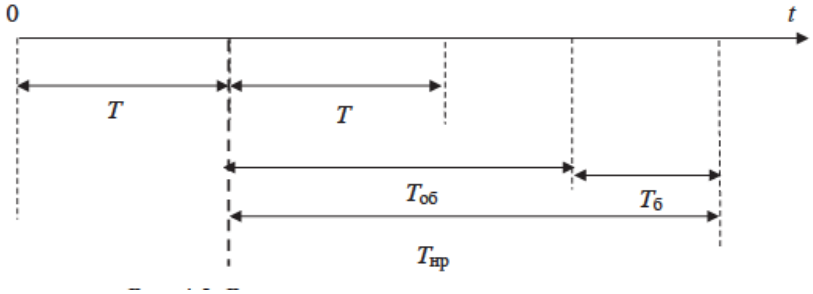


Рис. 3.2 - Временная диаграмма процесса контроля и обнаружения НСД:

$T$ — период опроса датчиков; $T_{об}$ — время передачи сигнала и обнаружения НСД; $T_б$ — время блокировки доступа; $T_{нр}$ — время нарушения

Из рис. 3.2 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 $P1$, то

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

В случае б), когда $T < T_{нр} < T_{об} + T$, несанкционированный доступ 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 доступа через $P_2$, то

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

Для более полного формального представления прочности преграды в виде системы обнаружения и блокировки несанкционированного доступа 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; $t$ — рассматриваемый интервал времени функционирования системы обнаружения и блокировки.

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

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

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

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).

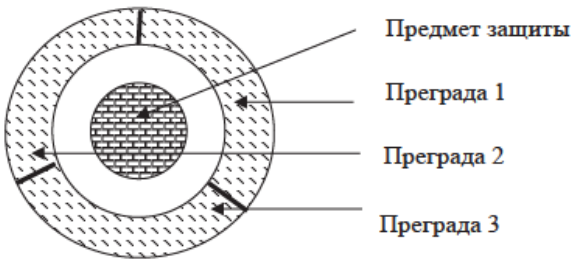


Рис. 3.3 - Модель многозвенной защиты

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.

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; $P_{оk}$ — 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: $P_{зи0} = P_{зи1} \cdot P_{зи2} \cdot \ldots P_{зиi} (1 — P_{о1}) (1 — P_{о2}) (1 — P_{о3}) \ldots (1 — P_{оk})$.

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. Дополнительные преграды должны перекрывать то же количество или более возможных каналов несанкционированного доступа, 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

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

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

При расчете суммарной прочности многоуровневой защиты суммируются прочности отдельных уровней.

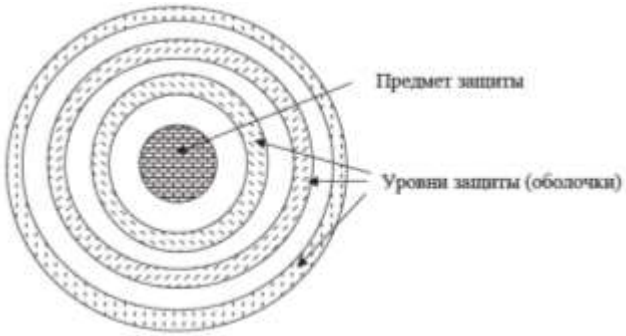


Рис. 3.4 - Модель многоуровневой защиты

ВЫВОДЫ

· Система защиты информации должна предусматривать защиту 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 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, является важной составляющей успешного проведения анализа риска и определения требований к составу и характеристикам системы защиты.

## 4 Определение и основные способы несанкционированного доступа. Методы защиты от НСД. Организационные методы защиты от НСД

*Определение и основные способы несанкционированного доступа*

В соответствии с определением несанкционированный доступ является одним из видов утечки информации.

Как уже было сказано выше, несанкционированным доступом к информации (НСД), согласно руководящим документам Гостехкомиссии, является доступ к информации, нарушающий установленные правила разграничения доступа.

НСД может носить случайный или преднамеренный характер.

В результате НСД чаще всего реализуется угроза конфиденциальности информации, однако целью злоумышленника может быть и реализация других видов угроз (целостности информации, раскрытия параметров системы).

Для преднамеренного НСД используются как общедоступные, так и скрытые способы и средства.

Такими способами являются:

· инициативное сотрудничество (предательство);

· склонение к сотрудничеству (подкуп, шантаж);

· подслушивание переговоров самыми различными путями;

· негласное ознакомление со сведениями, составляющими тайну;

· хищение, копирование, подделка, уничтожение;

· незаконное подключение к каналам и линиям связи и передачи данных; · перехват (акустический или радиоперехват, в том числе и за счет побочных электромагнитных излучений и наводок);

· визуальное наблюдение, фотографирование;

· сбор и аналитическая обработка детальной информации или производственных отходов.

К основным способам НСД в информационных системах относятся:

· непосредственное обращение к объектам доступа;

· создание программных и технических средств, выполняющих обращение к объектам доступа в обход средств защиты; · модификация средств защиты, позволяющая осуществить НСД;

· внедрение в технические средства информационной системы программных или технических механизмов, нарушающих предполагаемую структуру и функции системы и позволяющих осуществить НСД.

Зная совокупность источников информации, возможные каналы утечки охраняемых сведений и многообразие способов несанкционированного доступа к источникам, можно приступать к выработке мероприятий по защите.

*Методы защиты от НСД*

Можно выделить несколько обобщенных категорий методов защиты от НСД, в частности:

· организационные (в т. ч. административные);

· технологические (или инженерно-технические);

· правовые;

· финансовые;

· морально-этические (или социально-психологические).

К первой категории относятся меры и мероприятия, регламентируемые внутренними инструкциями организации, эксплуатирующей информационную систему. Пример такой защиты — присвоение грифов секретности документам и материалам, хранящимся в отдельном помещении, и контроль доступа к ним сотрудников.

Вторую категорию составляют механизмы защиты, реализуемые на базе программно-аппаратных средств, например, систем идентификации и аутентификации или охранной сигнализации.

Третья категория включает меры контроля за исполнением нормативных актов общегосударственного значения, механизмы разработки и совершенствования нормативной базы, регулирующей вопросы защиты информации.

Финансовые методы защиты предполагают введение специальных доплат при работе с защищаемой информацией, а также систему вычетов и штрафов за нарушение режимных требований.

Морально-этические методы не носят обязательного характера, однако являются достаточно эффективными при борьбе с внутренними нарушителями.

Реализуемые на практике методы, как правило, сочетают в себе элементы нескольких из перечисленных категорий. Так, управление доступом в помещения может представлять собой взаимосвязь организационных (выдача допусков и ключей) и технологических (установку замков и систем сигнализации) способов защиты.

*Организационные методы защиты от НСД*

Эффективная защита информации возможна при обязательном выполнении ряда условий:

· единство в решении производственных, коммерческих, финансовых и режимных вопросов;

· координация мер безопасности между всеми заинтересованными подразделениями предприятия;

· научная оценка информации и объектов, подлежащих классификации (защите);

разработка режимных мер до начала проведения режимных работ;

· персональная ответственность (в том числе и материальная) руководителей всех уровней, исполнителей, участвующих в закрытых работах, за обеспечение сохранности тайны и поддержание на должном уровне режима охраны проводимых работ;

· включение основных обязанностей рабочих, специалистов и администрации по соблюдению конкретных требований режима в коллективный договор, контракт, трудовое соглашение, правила трудового распорядка;

· организация специального делопроизводства, порядка хранения, перевозки носителей тайны; введение соответствующей маркировки документов и других носителей закрытых сведений;

· формирование списка лиц, уполномоченных руководителем предприятия классифицировать информацию и объекты, содержащие конфиденциальные сведения;

· оптимальное ограничение числа лиц, допускаемых к защищаемой информации;

· наличие единого порядка доступа и оформления пропусков;

· выполнение требований по обеспечению сохранения защищаемой информации при проектировании и размещении специальных помещений, в процессе опытно-конструкторской разработки, испытаний и производства изделий, сбыта, рекламы,

подписания контрактов, при проведении особо важных совещаний, в ходе использования технических средств обработки, хранения и передачи информации и т. п.;

· организация взаимодействия с государственными органами власти, имеющими полномочия по контролю определенных видов деятельности предприятий и фирм;

· наличие охраны, пропускного и внутриобъектового режимов;

· плановость разработки и осуществления мер по защите информации, систематический контроль за эффективностью принимаемых мер;

· создание системы обучения исполнителей правилам обеспечения сохранности информации.

## 5 Инженерно-технические методы защиты от НСД. Построение систем защиты от угрозы утечки по техническим каналам. Идентификация и аутентификация

*Инженерно-технические методы защиты от НСД. Построение систем защиты от угрозы утечки по техническим каналам*

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:

· несоблюдение персоналом норм, требований, правил эксплуатации;

· ошибки в проектировании системы и систем защиты;

· ведение противостоящей стороной технической и агентурной разведок.

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).

*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 или вне ее.

При выявлении каналов утечки информации необходимо рассматривать всю совокупность элементов системы, включающую основное оборудование технических средств обработки информации, 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, 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, использование производственных и технологических отходов, визуальный съем информации с монитора и принтера, несанкционированное копирование и т. п.

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

· 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 системы, 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.

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 средств вычислительной техники). 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.

*Идентификация и аутентификация*

К категории технологических методов защиты от НСД относятся идентификация и аутентификация.

Под безопасностью (стойкостью) системы идентификации и аутентификации будем понимать гарантированность того, что злоумышленник не способен пройти аутентификацию от имени другого пользователя. В этом смысле, чем выше стойкость системы аутентификации, тем сложнее злоумышленнику решить указанную задачу. Система идентификации и аутентификации является одним из ключевых элементов инфраструктуры защиты от НСД любой информационной системы. Различают три группы методов аутентификации, основанных на наличии у пользователей:

· индивидуального объекта заданного типа;

· индивидуальных биометрических характеристик;

· знаний некоторой известной только пользователю и проверяющей стороне информации.

К первой группе относятся методы аутентификации, предполагающие использование удостоверений, пропуска, магнитных карт и других носимых устройства, которые широко применяются для контроля доступа в помещения, а также входят в состав программно-аппаратных комплексов защиты от НСД к средствам вычислительной техники.

Во вторую группу входят методы аутентификации, основанные на применении оборудования для измерения и сравнения с эталоном заданных индивидуальных характеристик пользователя: тембра голоса, отпечатков пальцев, структуры радужной

оболочки глаза и др. Такие средства позволяют с высокой точностью аутентифицировать обладателя конкретного биометрического признака, причем «подделать» биометрические параметры практически невозможно.

Последнюю группу составляют методы аутентификации, при которых используются пароли. По экономическим причинам они включаются в качестве базовых средств защиты во многие программно-аппаратные комплексы защиты информации. Все современные операционные системы и многие приложения имеют встроенные механизмы парольной защиты.

Если в процедуре аутентификации участвуют только две стороны, устанавливающие подлинность друг друга, такая процедура называется непосредственной аутентификацией. Если же в процессе аутентификации участвуют не только эти стороны, но и другие, вспомогательные, говорят об аутентификации с участием доверенной стороны. Третью сторону называют сервером аутентификации или арбитром.

Выбирая тот или иной протокол аутентификации, необходимо определить, какая именно аутентификация требуется — односторонняя или взаимная, нужно ли использовать доверенное третье лицо и если да, то какая из сторон — претендент или верификатор — будет с ним взаимодействовать. Протоколы без- диалоговой аутентификации часто осуществляют еще и контроль целостности данных.

## 6 Основные направления и цели использования криптографических методов. Защита от угрозы нарушения конфиденциальности на уровне содержания информации.

*Основные направления и цели использования криптографических методов*

При построении защищенных систем роль криптографических методов для решения различных задач информационной безопасности трудно переоценить. Криптографические методы в настоящее время являются базовыми для обеспечения надежной аутентификации сторон информационного обмена, защиты информации в транспортной подсистеме, подтверждения целостности объектов информационной системы и т. д.

Проблемой защиты информации путем ее преобразования занимается криптология (лат. kryptos — тайный, logos — наука). Криптология разделяется на два направления — криптографию и криптоанализ. Цели этих направлений прямо противоположны.

Криптография занимается поиском и исследованием математических методов преобразования информации. Криптография дает возможность преобразовать информацию таким образом, что ее прочтение (восстановление) возможно только при знании ключа.

Сфера интересов криптоанализа — исследование возможности расшифровывания нформации без знания ключей.

Основные направления и цели использования криптографических методов: · передача конфиденциальной информации по каналам связи (например, электронная почта); · обеспечение достоверности и целостности информации; · установление подлинности передаваемых сообщений; · хранение информации (документов, баз данных) на носителях в зашифрованном виде; · выработка информации, используемой для идентификации и аутентификации субъектов, пользователей и устройств;

· выработка информации, используемой для защиты аутентифицирующих элементов защищенной системы.

В качестве информации, подлежащей шифрованию и дешифрованию, будут рассматриваться тексты, построенные на некотором алфавите.

*Алфавит* — конечное множество используемых для кодирования информации знаков.

*Текст* — упорядоченный набор из элементов алфавита.

В качестве примеров алфавитов, используемых в современных информационных системах, можно привести следующие: · алфавит Z33–32 буквы русского алфавита и пробел; · алфавит Z256 — символы, входящие в стандартные коды ASCII и КОИ-8; ·

бинарный алфавит — Z2 = {0,1}; · восьмеричный алфавит или шестнадцатеричный алфавит; *Шифрование* — преобразовательный процесс: исходный текст, который носит также название открытого текста, заменяется шифрованным текстом (рис. 6.1).

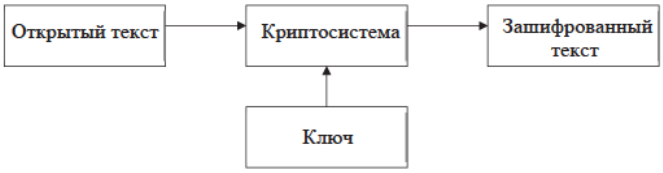


Рис. 6.1. Шифрование

*Дешифрование* — обратный шифрованию процесс. На основе ключа шифрованный текст преобразуется в исходный (рис. 6.2).

*Ключ* — информация, необходимая для беспрепятственного шифрования и дешифрования текстов. Обычно ключ представляет собой последовательный ряд букв алфавита.

Криптосистемы разделяются на симметричные и ассиметричные (с открытым ключом).


Рис. 6.2. Дешифрование

В *симметричных криптосистемах* и для шифрования, и для дешифрования используется один и тот же ключ: источник зашифровывает открытый текст на секретном ключе К, а приемник расшифровывает шифртекст на секретном ключе К*.

Обычно К = К*.

В *ассиметричных системах (системах с открытым ключом)* используются два ключа — открытый и закрытый, которые математически связаны друг с другом. Информация шифруется с помощью открытого ключа, который доступен всем желающим, а расшифровывается с помощью закрытого ключа, известного только получателю сообщения или наоборот.

*Криптостойкостью* называется характеристика шифра, определяющая его стойкость к дешифрованию без знания ключа (т. е. криптоанализу).

В зависимости от исхода криптоанализа все алгоритмы шифрования можно разделить на три группы.

К первой группе относятся совершенные шифры, заведомо не поддающиеся дешифрованию (при правильном использовании). Примером такого шифра является шифр гаммирования случайной равновероятной гаммой.

Во вторую группу входят шифры, допускающие неоднозначное дешифрование. Например, такая ситуация возникает, если зашифровать с помощью шифра простой замены очень короткое сообщение.

Основная масса используемых шифров относится к третьей группе и может быть в принципе однозначно дешифрована.

Сложность дешифрования шифра из этой группы будет определяться трудоемкостью используемого алгоритма дешифрования. Следовательно, для оценки стойкости такого шифра необходимо рассмотреть все известные алгоритмы дешифрования и выбрать из них имеющий минимальную трудоемкость, т. е. тот, который работает в данном случае быстрее всех остальных.

Трудоемкость этого алгоритма и будет характеризовать стойкость исследуемого шифра.

Удобнее всего измерять трудоемкость алгоритма дешифрования в элементарных операциях, но более наглядным параметром является время, необходимое для вскрытия шифра (при этом необходимо указывать технические средства, которые доступны криптоаналитику). Не следует забывать, что вполне возможно существование неизвестного на данный момент алгоритма, который может значительно снизить вычисленную стойкость шифра. К большому сожалению работчиков шифросистем, строго доказать с помощью математических методов невозможность существования простых алгоритмов дешифрования удается чрезвычайно редко. Очень хорошим результатом в криптографии является доказательство того, что сложность решения задачи дешифрования исследуемого шифра эквивалентна сложности решения какой-нибудь известной математической задачи. Такой вывод хотя и не дает 100 % гарантии, но позволяет надеяться, что существенно понизить оценку стойкости шифра в этом случае будет очень непросто.

К средствам криптографической защиты информации (СКЗИ) относятся: · аппаратные; · программно-аппаратные; · программные средства.

Предполагается, что СКЗИ используются в некоторой информационной системе совместно с механизмами реализации и гарантирования политики безопасности.

Можно говорить о том, что СКЗИ производят защиту объектов на семантическом уровне. В то же время объекты-параметры криптографического преобразования являются полноценными объектами информационной системы и могут быть объектами некоторой политики безопасности (например, ключи шифрования могут и должны быть защищены от НСД, открытые ключи для проверки цифровой подписи — от изменений и т. д.).

Основные причины нарушения безопасности информации при ее обработке СКЗИ:

1. Утечка информации по техническим каналам.
2. Неисправности в элементах СКЗИ.
3. Работа совместно с другими программами: непреднамеренное и преднамеренное влияние (криптовирусы).
4. Воздействие человека.

В связи с этим помимо встроенного контроля за пользователем, необходимо отслеживание правильности разработки и использования средств защиты с применением организационных мер.

Процесс синтеза и анализа СКЗИ отличается высокой сложностью и трудоемкостью, поскольку необходим всесторонний учет влияния перечисленных выше угроз на надежность реализации СКЗИ. В связи с этим практически во всех странах, обладающих развитыми криптографическими технологиями, разработка СКЗИ относится к сфере государственного регулирования.

Государственное регулирование включает, как правило, лицензирование деятельности, связанной с разработкой и эксплуатацией криптографических средств, сертификацию СКЗИ и стандартизацию алгоритмов криптографических преобразований.

В России в настоящее время организационно-правовые и научно-технические проблемы синтеза и анализа СКЗИ находятся в компетенции ФСБ.

Правовая сторона разработки и использования СКЗИ регламентируется в основном указом Президента Российской Федерации от 03.04.95 № 334 с учетом принятых ранее законодательных и нормативных актов РФ.

Дополнительно учитываемой законодательной базой являются законы «О федеральных органах правительственной связи и информации», «О государственной тайне», «Об информации, информационных технологиях и о защите информации», «О сертификации продукции и услуг».

В настоящее время шифрование является единственным надежным средством защиты при передаче информации.

*Защита от угрозы нарушения конфиденциальности на уровне содержания информации*

Существуют различные методы защиты конфиденциальности информации на уровне содержания.

Рассмотрим ситуацию, когда злоумышленнику удалось получить доступ к синтаксическому представлению конфиденциальной информации, т. е. он имеет перед собой последовательность знаков некоторого языка, удовлетворяющую формальным правилам нотации. Данная ситуация может возникнуть, например, тогда, когда удалось дешифровать файл данных и получить текст, который может рассматриваться как осмысленный. В этом случае для сокрытия истинного содержания сообщения могут применяться различные приемы, суть которых сводится к тому, что в соответствие одной последовательности знаков или слов одного языка ставятся знаки или слова другого.

В качестве примера можно привести шифр «Аве Мария», в кодовом варианте которого каждому слову, а порой и фразе ставятся в соответствие несколько слов явной религиозной тематики, в результате чего сообщение выглядит как специфический текст духовного содержания. Обычный жаргон также может иллюстрировать применяемые в повседневной практике подходы к сокрытию истинного смысла сообщений.

Другим направлением защиты является использование стеганографии. Слово «стеганография» в переводе с греческого буквально означает «тайнопись». К ней относится огромное множество секретных средств связи, таких как невидимые чернила, микрофотоснимки, условное расположение знаков (применяемое в сигнальной агентурной связи), цифровые подписи, тайные каналы и средства связи на плавающих частотах.

Вот какое определение предлагает Маркус Кун: «Стегано- графия — это искусство и наука организации связи таким способом, который скрывает собственно наличие связи. В отличие от криптографии, где неприятель имеет возможность обнаруживать, перехватывать и декодировать сообщения — при том, что ему противостоят определенные меры безопасности, гарантированные той или иной криптосистемой, — методы стеганографии позволяют встраивать секретные сообщения в безобидные послания так, чтобы нельзя было даже подозревать существования подтекста».

Применительно к компьютерным технологиям можно сказать, что стеганография использует методы размещения файла- сообщения в файле- «контейнере», изменяя файл-«контейнер» таким образом, чтобы сделанные изменения были практически незаметны. Большинство из компьютерных стеганографических приемов объединяет методология изменения наименьшего значимого бита (Least Significant Bits-LSB), который считается «шумящим», т. е. имеющим случайный характер в отдельных байтах файла-«контейнера».

На практике в большинстве случаев открытый контейнер не содержит бесполезных данных, которые могут быть использованы для модификации. Вместо этого контейнерные файлы естественно содержат различные уровни шума, который при ближайшем рассмотрении, за исключением остальной части байта, может являться произвольной величиной. Звуковой (.WAV) файл, например, содержит по большей части неслышный шум фона на уровне LSB; 24-битовый графический образ будет содержать изменения цвета, которые почти незаметны человеческому глазу.

ВЫВОДЫ

· Эффективная защита от НСД возможна только при сочетании различных методов: организационных, технических, нормативно-правовых.

· Для перекрытия каналов несанкционированного доступа к информации большое значение имеет построение систем идентификации и аутентификации, позволяющих ограничить доступ к защищаемой информации. Подобные системы используются как при контроле физического доступа (биометрическая аутентификация, аутентификация с использованием определенного объекта), так и при контроле доступа к ресурсам и данным (парольные системы).

· В настоящее время криптографические методы защиты информации от несанкционированного доступа являются единственным надежным средством защиты при

передаче информации по каналам связи. Целесообразно использовать криптографическую защиту при хранении информации, что позволит в сочетании с мерами по ограничению доступа предотвратить несанкционированный доступ к информации.