РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ ГУМАНИТАРНЫЙ УНИВЕРСИТЕТ
ИНСТИТУТ ИНФОРМАЦИОННЫХ НАУК И ТЕХНОЛОГИЙ БЕЗОПАСНОСТИ
Кафедра комплексной защиты информации

Митюшин Дмитрий Алексеевич

Информационные технологии. Администрирование подсистем защиты информации

Тема 2. Угрозы безопасности информационной системы

Вопросы:

1. *Угрозы безопасности информации и уязвимости информационных систем*
2. *Утечка и несанкционированный доступ к информации*
3. *Подсистемы системы защиты информации*

Литература

1. Основы защиты информации: учебное пособие. Изд. 5-е, перераб. И доп. – Томск: В-Спектр, 2011. – 244 с. //Шелупанов
2. Гатчин Ю.А., Климова Е.В. Введение в комплексную защиту объектов информатизации: учебное пособие. – СПб: НИУ ИТМО, 2011. – 112 с.
3. Гришина Н. В. Организация комплексной системы защиты информации. – М.: Гелиос АРВ, 2007. – 256 с, ил.

1. Угрозы безопасности информации и уязвимости ИС

1.1. Основные термины и определения

Для обеспечения информационной безопасности необходимо постоянно поддерживать следующие свойства информации и систем её обработки:

- ***доступность информации*** – такое свойство системы (инфраструктуры, средств и технологии обработки, в которой циркулирует информация), которое характеризует её способность обеспечивать своевременный доступ субъектов к интересующей их информации и соответствующим автоматизированным службам (готовность к обслуживанию поступающих от субъектов) запросов всегда, когда в обращении к ним возникает необходимость;
- ***конфиденциальность информации*** – такую субъективно определяемую (приписываемую) характеристику (свойство) информации, которая указывает на необходимость введения ограничений на круг субъектов, имеющих доступ к данной информации, и обеспечиваемую способностью системы (инфраструктуры) сохранять указанную информацию втайне от субъектов, не имеющих прав на доступ к ней.

Объективные предпосылки подобного ограничения доступности информации для одних субъектов заключены в необходимости защиты законных интересов других субъектов информационных отношений.

1. Угрозы безопасности информации и уязвимости ИС

1.1. Основные термины и определения

Под ***безопасностью автоматизированной системы*** (системы обработки информации, компьютерной системы) следует понимать защищённость всех её компонентов (технических средств, программного обеспечения, данных, пользователей и персонала) от разного рода нежелательных воздействий.

Безопасность любого компонента (ресурса) АС складывается из обеспечения трёх его характеристик: конфиденциальности, целостности и доступности.

Конфиденциальность компонента (ресурса) АС заключается в том, что он доступен только тем субъектам (пользователям, программам, процессам), которым предоставлены на то соответствующие полномочия.

Целостность компонента (ресурса) АС предполагает, что он может быть модифицирован только субъектом, имеющим для этого соответствующие права. Целостность является гарантией корректности (неизменности, работоспособности) компонента в любой момент времени.

1. Угрозы безопасности информации и уязвимости ИС

1.1. Основные термины и определения

Доступность компонента (ресурса) АС означает, что имеющий соответствующие полномочия субъект может в любое время без особых проблем получить доступ к необходимому компоненту системы.

Кроме того, необходимо дать определения таким понятиям как угрозы, уязвимости и атаки на компоненты АС.

Угроза – это потенциально возможное событие, явление или процесс, которое посредством воздействия на компоненты информационной системы может привести к нанесению ущерба.

Уязвимость – это любая характеристика или свойство информационной системы, использование которой нарушителем может привести к реализации угрозы.

Атака – это любое действие нарушителя, которое приводит к реализации угрозы путём использования уязвимостей информационной системы.

1. Угрозы безопасности информации и уязвимости ИС

1.2. Классификация угроз

Информационные системы подвержены широкому кругу угроз.

Все угрозы условно можно разделить на две большие группы:

1. угрозы утечки информации по техническим каналам связи и
2. угрозы несанкционированного доступа к информации.

Первая группа угроз включает в себя угрозы утечки акустической (речевой), видовой информации, а так же утечки по каналу ПЭМИН.

Вторая группа угроз характеризуется различными способами реализации несанкционированного получения доступа к информации, в том числе с использованием возможностей компьютерных сетей.

В настоящее время рассматривается достаточно обширный перечень угроз информационной безопасности АС, насчитывающий сотни пунктов. Наиболее характерные и часто реализуемые из них следующие:

- несанкционированное копирование носителей информации;
- неосторожные действия, приводящие к разглашению конфиденциальной информации, или делающие её общедоступной;
- игнорирование организационных ограничений (установленных правил) при определении ранга системы.

1. Угрозы безопасности информации и уязвимости ИС

1.2. Классификация угроз

Классификация всех возможных угроз информационной безопасности АС может быть проведена по ряду базовых признаков.

По природе возникновения:

- Естественные угрозы – угрозы, вызванные воздействиями на АС и её компоненты объективных физических процессов или стихийных природных явлений, независящих от человека.
- Искусственные угрозы – угрозы ИБ АС, вызванные деятельностью человека.

По степени преднамеренности проявления:

- Угрозы случайного действия и/или угрозы, вызванные ошибками или халатностью персонала.
- Угрозы преднамеренного действия.

По непосредственному источнику угроз:

- Угрозы, непосредственным источником которых является природная среда.
- Угрозы, непосредственным источником которых является человек.
- Угрозы, непосредственным источником которых являются санкционированные программно-аппаратные средства.
- Угрозы, непосредственным источником которых являются несанкционированные программно-аппаратные средства.

1. Угрозы безопасности информации и уязвимости ИС

1.2. Классификация угроз

По положению источника угроз:

- Угрозы, источник которых расположен вне контролируемой зоны территории (помещения), на которой находится АС.
- Угрозы, источник которых расположен в пределах контролируемой зоны территории (помещения), на которой находится АС.
- Угрозы, источник которых имеет доступ к периферийным устройствам АС (терминалам).
- Угрозы, источник которых расположен в АС.

По степени зависимости от активности АС:

- Угрозы, которые могут проявляться независимо от активности АС.
- Угрозы, которые могут проявляться только в процессе автоматизированной обработки данных.

По степени воздействия на АС:

- Пассивные угрозы, которые при реализации ничего не меняют в структуре и содержании АС.
- Активные угрозы, которые при воздействии вносят изменения в структуру и содержание АС.

1. Угрозы безопасности информации и уязвимости ИС

1.2. Классификация угроз

По этапам доступа пользователей или программ к ресурсам АС:

- Угрозы, которые могут проявляться на этапе доступа к ресурсам АС.
- Угрозы, которые могут проявляться после разрешения доступа к ресурсам.

По способу доступа к ресурсам АС:

- Угрозы, направленные на использование прямого стандартного пути доступа к ресурсам АС.
- Угрозы, направленные на использование скрытого нестандартного пути доступа к ресурсам АС.

По текущему месту расположения информации, хранимой и обрабатываемой в АС:

- Угрозы доступа к информации на внешних запоминающих устройствах.
- Угрозы доступа к информации в оперативной памяти.
- Угрозы доступа к информации, циркулирующей в линиях связи.
- Угрозы доступа к информации, отображаемой на терминале или печатаемой на принтере.

1. Угрозы безопасности информации и уязвимости ИС

1.2. Классификация угроз

В соответствии с существующими подходами, принято считать, что информационная безопасность АС обеспечена в случае, если для любых информационных ресурсов в системе поддерживается определённый уровень конфиденциальности (невозможности несанкционированного получения какой-либо информации), целостности (невозможности несанкционированной или случайной её модификации) и доступности (возможности за разумное время получить требуемую информацию).

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

Угроза нарушения конфиденциальности заключается в том, что информация становится известной тому, кто не располагает полномочиями доступа к ней. В терминах компьютерной безопасности 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».

1. Угрозы безопасности информации и уязвимости ИС

1.2. Классификация угроз

Угроза нарушения целостности включает в себя любое умышленное изменение 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 отказа служб возникает всякий раз, когда в результате преднамеренных действий, предпринимаемых другим пользователем или злоумышленником, блокируется доступ к некоторому ресурсу вычислительной системы. Реально блокирование может быть постоянным – запрашиваемый ресурс никогда не будет получен, или оно может вызывать только задержку запрашиваемого ресурса, достаточно долгую для того, чтобы он стал бесполезным. В этих случаях говорят, что ресурс исчерпан.

1. Угрозы безопасности информации и уязвимости ИС

1.2. Классификация угроз

В информационных системах на базе автономного АРМ, а также в ИС не имеющих подключения к сетям общего пользования, угрозы возникают в связи с действиями нарушителя, имеющего доступ в ИС, т.е. внутреннего нарушителя.

В ИС, имеющих подключение к сетям общего пользования, угрозы возникают в связи с действиями нарушителя, как имеющего доступ в ИС, так и не имеющего такового доступа, т.е. к внутренним нарушителям добавляются внешние.

В ИС на базе автономного АРМ возможны все виды угроз, за исключением угроз, связанных с реализацией протоколов сетевого взаимодействия и каналов передачи данных.

В ИС на базе локальных, распределённых сетей, а так же имеющих подключение к сетям общего пользования дополнительно возникают угрозы, связанные с реализацией протоколов сетевого взаимодействия и каналов передачи данных.

1. Угрозы безопасности информации и уязвимости ИС

1.2. Классификация угроз

Например, для распределённых ИС, имеющих подключение к сетям общего пользования, возможна реализация следующих угроз:

- угрозы «Анализа сетевого трафика» с перехватом передаваемой из ИС и принимаемой в ИС из внешних сетей информации;
- угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций, топологии сети, открытых портов и служб, открытых соединений и др.;
- угрозы внедрения ложного объекта как в информационной системе, так и во внешних сетях;
- угрозы подмены доверенного объекта;
- угрозы навязывания ложного маршрута путём несанкционированного изменения маршрутно-адресных данных как внутри сети, так и во внешних сетях;
- угрозы выявления паролей;
- угрозы типа «Отказ в обслуживании»;
- угрозы удалённого запуска приложений;
- угрозы внедрения по сети вредоносных программ.

1. Угрозы безопасности информации и уязвимости ИС

1.3. Классификация уязвимостей

Из приведённых выше определений угроз, уязвимостей и атак видно, что производя определённую атаку, нарушитель обязательно использует некоторую уязвимость информационной системы. Иначе говоря, если нет уязвимости, то невозможна и атака, её использующая.

Поэтому одним из важнейших механизмов защиты является процесс поиска и устранения уязвимостей информационной системы.

Прежде всего, рассмотрим возможные варианты (критерии) классификации уязвимостей IP-сетей. Такая классификация нужна, например, для создания упорядоченной базы данных уязвимостей, которая может пополняться по мере обнаружения новых уязвимостей.

Источники возникновения уязвимостей

Часть уязвимостей закладывается ещё на этапе проектирования. В качестве примера можно привести сервис TELNET, в котором имя пользователя и пароль передаются по сети в открытом виде. Это явный недостаток, заложенный на этапе проектирования. Некоторые уязвимости подобного рода трудно назвать недостатками, скорее это особенности проектирования. Например, особенность технологии Ethernet – общая среда передачи.

1. Угрозы безопасности информации и уязвимости ИС

1.3. Классификация уязвимостей

Другая часть уязвимостей возникает на этапе реализации (программирования). К таким уязвимостям относятся, например, ошибки программирования стека TCP/IP, приводящие к отказу в обслуживании. Сюда же следует отнести и ошибки при написании приложений, приводящие к переполнению буфера и т.п.

И, наконец, уязвимости могут быть следствием ошибок, допущенных в процессе эксплуатации информационной системы. Сюда относятся неверное конфигурирование операционных систем, протоколов и служб, использование нестойких паролей пользователей, паролей учётных записей «по умолчанию» и др.

Классификация уязвимостей по уровню в инфраструктуре АС

Следующий вариант классификации уязвимостей – по их уровню в информационной инфраструктуре организации. Это наиболее наглядный вариант классификации, т.к. он показывает, что конкретно уязвимо.

- *К уровню сети* относятся уязвимости сетевых протоколов – стека TCP/IP, протоколов NetBEUI, IPX/SPX (например, аутентификация узлов на основе назначаемого IP-адреса в протоколе IP).
- *Уровень операционной системы* охватывает уязвимости Windows, UNIX, Novell и т.д., т.е. конкретной операционной системы.
- На *уровне баз данных* находятся уязвимости конкретных СУБД – Oracle, MS SQL, Sybase и др.

1. Угрозы безопасности информации и уязвимости ИС

1.3. Классификация уязвимостей

- К *уровню приложений* относятся уязвимости программного обеспечения WEB, SMTP серверов, клиентских программ и т.п.
- *Персонал и пользователи* системы также уязвимы. Например, один из путей внедрения вредоносных программ – это провоцирование пользователей на запуск присланных по электронной почте приложений.

Классификация уязвимостей по степени риска

Этот вариант (критерий) классификации уязвимостей является достаточно субъективным (условным). Если придерживаться взгляда компании Internet Security Systems, можно выделить уязвимости трёх уровней риска:

- *Высокий уровень риска* – уязвимости, позволяющие атакующему получить непосредственный доступ к узлу с правами суперпользователя или в обход межсетевых экранов или иных средств защиты (полный контроль над атакуемым объектом).
- *Средний уровень риска* – Уязвимости, позволяющие атакующему получить информацию, которая с высокой степенью вероятности позволит в дальнейшем получить полный контроль над объектом и доступ к любым его ресурсам.
- *Низкий уровень риска* – Уязвимости, позволяющие злоумышленнику осуществлять сбор критичной информации о системе.

1. Угрозы безопасности информации и уязвимости ИС

1.4. Классификация атак

Также как и уязвимости, атаки можно классифицировать по различным признакам.

Наиболее важно для понимания сути происходящих атак представлять механизмы их реализации. Основными механизмами реализации атак являются:

- *пассивное прослушивание* – состоит в перехвате трафика сетевого сегмента
- *подозрительная активность* – сканирование портов (служб) объекта атаки, попытки подбора пароля
- *бесполезное расходование вычислительного ресурса* – исчерпание ресурсов атакуемого узла или группы узлов, приводящее к снижению производительности, зависанию службы или операционной системы (переполнение очереди запросов на соединение и т.п.)
- *нарушение навигации* (создание ложных объектов и маршрутов) – изменение маршрута сетевых пакетов, таким образом, чтобы они проходили через хосты и маршрутизаторы нарушителя, изменение таблиц соответствия условных Internet-имён и IP-адресов (атаки на DNS) и т.п.
- *выведение из строя* – посылка пакетов определённого типа на атакуемый узел, приводящая к отказу узла или работающей на нём службы (WinNuke и др.)
- *запуск приложений на объекте атаки* – выполнение враждебной программы в оперативной памяти объекта атаки (троянские кони, передача управления враждебной программе путём переполнения буфера, исполнение

1. Угрозы безопасности информации и уязвимости ИС

1.4. Классификация атак

Информацию об известных и новых обнаруживаемых уязвимостях можно найти в сети Интернет на сайтах, таких как:

Иностранные:

www.iss.net – компания Internet Security Systems;

www.cert.org – координационный центр CERT;

www.sans.org – институт системного администрирования, сетевых технологий и защиты;

www.ciae.org – группа реагирования на инциденты в области компьютерной безопасности;

www.securityfocus.com – информация об обнаруженных уязвимостях с подробными пояснениями и группой новостей и др.;

osvdb.org – открытая база данных уязвимостей.

Отечественные:

www.sreport.ru – база данных уязвимостей Интернет-серверов;

www.securitylab.ru – информация об уязвимостях различного системного и прикладного программного обеспечения.

1. Угрозы безопасности информации и уязвимости ИС

1.4. Классификация атак

Common Vulnerabilities and Exposures (CVE) – это список стандартных названий для общеизвестных уязвимостей. Основное назначение CVE – это согласование различных баз данных уязвимостей и инструментов, использующих такие базы данных. Например, одна и та же уязвимость может иметь различные названия в базе данных Internet Scanner и CyberCop Scanner .

Появление CVE – это результат совместных усилий известных мировых лидеров в области информационной безопасности: институтов, производителей ПО и т.д. Поддержку CVE осуществляет MITRE Corporation (www.mitre.org).

Процесс получения индекса CVE (CVE entry) начинается с обнаружения уязвимости. Затем уязвимости присваивается статус кандидата CVE и соответствующий номер (CVE candidate number). После этого происходит обсуждение кандидатуры при помощи CVE Editorial Board и вынесение решения о получении или неполучении индекса CVE .
Подробнее узнать о CVE и получить список CVE entry можно по адресу: **http://cve.mitre.org/cve** .

2. Утечка и несанкционированный доступ к информации

2.1. Утечка информации

Основными объектами защиты информации являются:

- Информационные ресурсы, содержащие сведения, связанные с государственной тайной и конфиденциальной информацией.
- Средства и информационные системы (средства вычислительной техники, сети и системы), программные средства (операционные системы, системы управления базами данных, прикладное программное обеспечение), автоматизированные системы управления, системы связи и передачи данных, технические средства приёма, передачи и обработки информации ограниченного доступа (звукозапись, звукоусиление, звуковоспроизведение, переговорные и телевизионные устройства, средства изготовления, тиражирование документов и другие технические средства обработки графической, смысловой и буквенно-цифровой информации), т.е. системы и средства, непосредственно обрабатывающие конфиденциальную информацию и информацию, относящуюся к категории государственной тайны. Эти средства и системы часто называют техническими средствами приёма, обработки и хранения информации (ТСПИ).

2. Утечка и несанкционированный доступ к информации

2.1. Утечка информации

Технические средства и системы, не входящие в состав ТСПИ, но территориально находящиеся в помещениях обработки секретной и конфиденциальной информации. Такие технические средства и системы называются вспомогательными техническими средствами и системами (ВТСС). К ним относятся: технические средства телефонной, громкоговорящей связи, системы пожарной и охранной сигнализации, радиотрансляции, часофикации, средства и системы передачи данных в системе радиосвязи, контрольно-измерительная аппаратура, электробытовые приборы и т.д., а также сами помещения, предназначенные для обработки информации ограниченного распространения.

ТСПИ можно рассматривать как систему, включающую стационарное оборудование, периферийные устройства, соединительные линии, распределительные и коммуникационные устройства, системы электропитания, системы заземления.

Технические средства, предназначенные для обработки конфиденциальной информации, включая помещения, в которых они размещаются, представляют ***объект ТСПИ***.

2. Утечка и несанкционированный доступ к информации

2.1. Утечка информации

Наибольший интерес с точки зрения образования каналов утечки информации представляют ТСПИ и ВТСС, имеющие выход за пределы ***контролируемой зоны*** (КЗ), т.е. зоны с пропускной системой. Кроме соединительных линий ТСПИ и ВТСС за пределы контролируемой зоны могут иметь выход проходящие через помещения посторонние проводники, не связанные с ТСПИ и ВТСС (рис. 1).

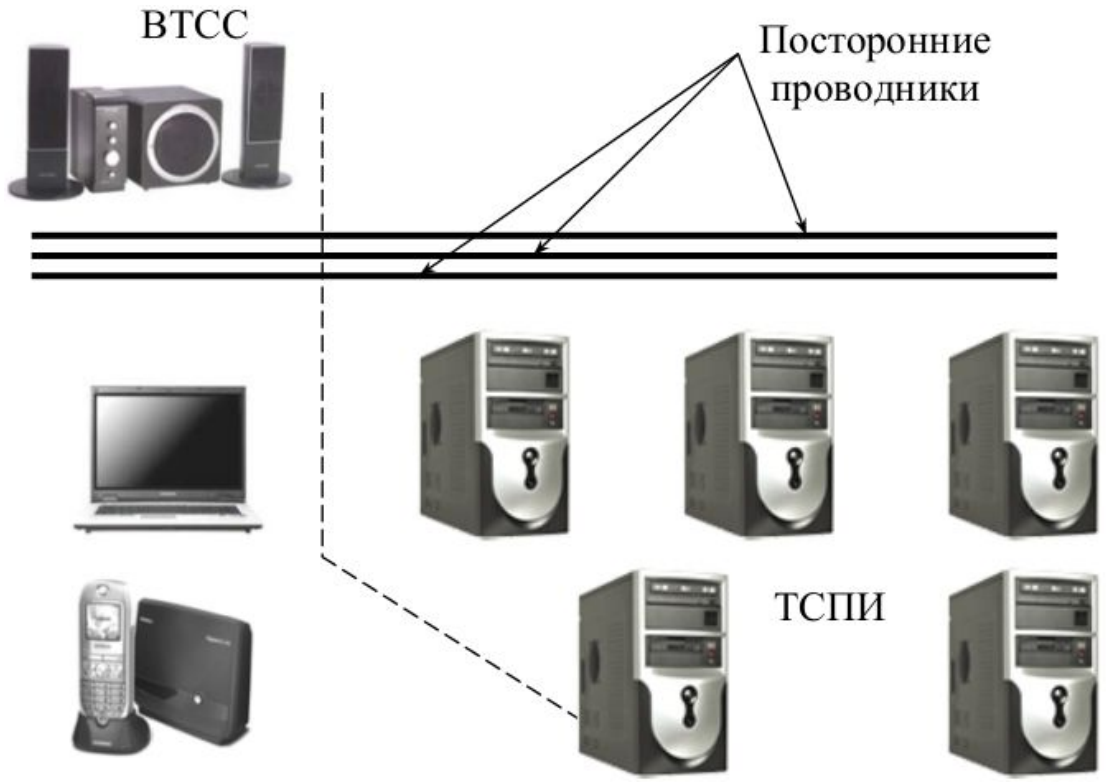

Рис. 1. Источники образования возможных каналов утечки информации

2. Утечка и несанкционированный доступ к информации

2.1. Утечка информации

Зона с возможностью перехвата разведывательным оборудованием побочных электромагнитных излучений, содержащих конфиденциальную информацию, называется ***опасной зоной***. Пространство вокруг ТСПИ, в котором на случайных антеннах наводится информационный сигнал выше допустимого уровня, называется ***опасной зоной 1***.

Случайными антеннами могут быть цепи ВТСС или посторонние проводники, воспринимающие побочные электромагнитные излучения от средств ТСПИ. Случайные антенны бывают сосредоточенными и распределёнными. Сосредоточенная случайная антенна представляет собой техническое средство с сосредоточенными параметрами (телефонный аппарат, громкоговоритель радиотрансляционной сети и т.д.). Распределённые случайные антенны образуют проводники с распределёнными параметрами: кабели, соединительные провода, металлические трубы.

Информационные сигналы могут быть электрическими, электромагнитными, акустическими и т.д. Они имеют в большинстве случаев колебательный характер, а информационными параметрами являются амплитуда, фаза, частота, длительность.

Перехват и измерения параметров сигналов осуществляют технические средства обработки информации и технические средства разведки (ТСР).

2. Утечка и несанкционированный доступ к информации

2.1. Утечка информации

Под техническим каналом утечки информации (ТКУИ) понимают совокупность объекта разведки, технического средства разведки (ТСР) и физической среды, в которой распространяется информационный сигнал (рис. 2). В сущности, под ТКУИ понимают способ получения с помощью ТСР разведывательной информации об объекте.

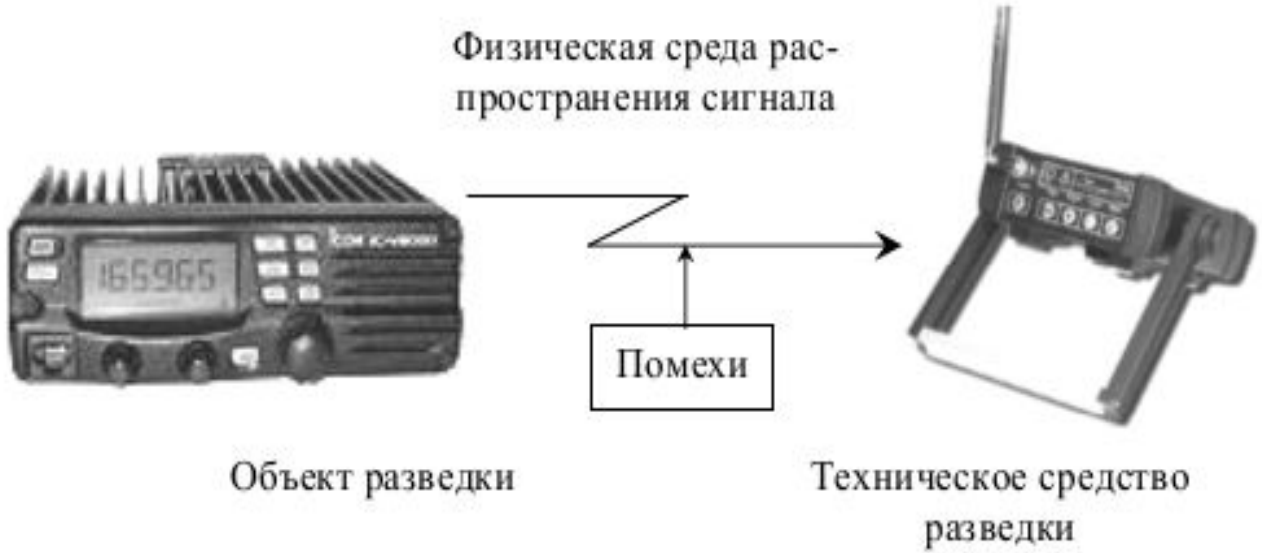

Рис. 2. Технический канал утечки информации (ТКУИ)

2. Утечка и несанкционированный доступ к информации

2.1. Утечка информации

В зависимости от физической природы сигналы распространяются в определённых физических средах.

Средой распространения могут быть газовые (воздушные), жидкостные (водные) и твёрдые среды. К таким средам относятся воздушное пространство, конструкции зданий, соединительные линии и токопроводящие элементы, грунт и т.п.

Противодействие промышленному и экономическому шпионажу является непрерывным и адекватным новым типам угроз процессом развития методов, средств и способов защиты информации.

Особенности технических каналов утечки информации определяются физической природой информационных сигналов и характеристиками среды распространения сигналов утекаемой информации. Ниже приведены некоторые особенности технических каналов утечки информации.

2. Утечка и несанкционированный доступ к информации

2.1. Утечка информации

Технические каналы утечки информации, обрабатываемой ТСПИ

1. Электромагнитные:
- электромагнитные излучения элементов ТСПИ;
- электромагнитные излучения на частотах работы ВЧ-генераторов ТСПИ;
- излучения на частотах самовозбуждения усилителей низкой частоты.

2. Электрические:
- наводки электромагнитных излучений элементов ТСПИ на посторонние проводники;
- просачивание информационных сигналов в линии электропитания;
- просачивание информационных сигналов в цепи заземления;
- съем информации с использованием закладных устройств.

3. Параметрические:
- перехват информации путём «высокочастотного облучения» ТСПИ.

4. Вибрационные:
- соответствие между распечатываемым символом и его акустическим образом.

2. Утечка и несанкционированный доступ к информации

2.1. Утечка информации

Технические каналы утечки информации при передаче её по каналам связи

1. Электромагнитные каналы:

- электромагнитные излучения передатчиков связи, модулированные информационным сигналом (прослушивание радиотелефонов, сотовых телефонов, радиорелейных линий связи).

2. Электрические каналы:

- подключение к линиям связи.

3. Индукционный канал:

- эффект возникновения вокруг высокочастотного кабеля электромагнитного поля при прохождении информационных сигналов.

4. Паразитные связи:

- паразитные ёмкостные, индуктивные и резистивные связи и наводки близко расположенных друг от друга линий передачи информации.

2. Утечка и несанкционированный доступ к информации

2.1. Утечка информации

Технические каналы утечки речевой информации

1. Акустические каналы:
• среда распространения – воздух.

2. Виброакустические каналы:
• среда распространения – ограждающие строительные конструкции.

3. Параметрические каналы:
• результат воздействия акустического поля на элементы схем, что приводит к модуляции высокочастотного сигнала информационным.

4. Акустоэлектрические каналы:
• преобразование акустических сигналов в электрические.

5. Оптико-электронный (лазерный) канал:
• облучение лазерным лучом вибрирующих поверхностей.

2. Утечка и несанкционированный доступ к информации

2.1. Утечка информации

Технические каналы утечки видовой информации

1. Наблюдение за объектами.
Для наблюдения днём применяются оптические приборы и телевизионные камеры. Для наблюдения ночью – приборы ночного видения, тепловизоры, телевизионные камеры.

2. Съёмка объектов.
Для съёмки объектов используются телевизионные и фотографические средства. Для съёмки объектов днём с близкого расстояния применяются портативные камуфлированные фотоаппараты и телекамеры, совмещённые с устройствами видеозаписи.

3. Съёмка документов.
Съёмка документов осуществляется с использованием портативных фотоаппаратов

2. Утечка и несанкционированный доступ к информации

2.2. Несанкционированный доступ к информации

Что такое НСД приводится в руководящем документе (РД) «Защита от НСД к информации. Термины и определения», утверждённом решением председателя Гостехкомиссии России от 30 марта 1992 г.

Установленные термины обязательны для применения во всех видах документации.

Для каждого понятия установлен один термин. Применение синонимов термина не допускается.

Для отдельных терминов даны (в скобках) краткие формы, которые разрешается применять в случаях, исключающих возможность их различного толкования.

Доступ к информации (***Доступ***) – ознакомление с информацией, её обработка, в частности, копирование, модификация или уничтожение информации.

Правила разграничения доступа (***ПРД***) – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа. По-английски – политики безопасности.

2. Утечка и несанкционированный доступ к информации

2.2. Несанкционированный доступ к информации

Санкционированный доступ к информации – доступ к информации, не нарушающий правила разграничения доступа.

Несанкционированный доступ к информации (***НСД***) – доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники (СВТ) или автоматизированными системами (АС).

Примечание. Под штатными средствами понимается совокупность программного, микропрограммного и технического обеспечения СВТ или АС.

Защита от несанкционированного доступа (***Защита от НСД***) – предотвращение или существенное затруднение НСД.

Субъект доступа (***Субъект***) – лицо или процесс, действия которого регламентируются правилами разграничения доступа.

Объект доступа (***Объект***) – единица информационного ресурса автоматизированной системы, доступ к которой регламентируется правилами разграничения доступа.

2. Утечка и несанкционированный доступ к информации

2.2. Несанкционированный доступ к информации

Классы защищённости СВТ и АС определяются соответствующими РД Гостехкомиссии.

Показатели защищённости СВТ применяются к общесистемным программным средствам и операционным системам (с учётом архитектуры ЭВМ).

Конкретные перечни показателей определяют классы защищённости СВТ. Уменьшение или изменение перечня показателей, соответствующего конкретному классу защищённости СВТ, не допускается.

Каждый показатель описывается совокупностью требований.

Дополнительные требования к показателю защищённости СВТ и соответствие этим дополнительным требованиям оговаривается особо.

Устанавливается семь классов защищённости СВТ от НСД. Самый низкий класс – седьмой, самый высокий – первый.

2. Утечка и несанкционированный доступ к информации

2.2. Несанкционированный доступ к информации

Классы подразделяются на четыре группы, отличающиеся качественным уровнем защиты:

- первая группа содержит только один седьмой класс;
- вторая группа характеризуется ***дискреционной*** защитой и содержит шестой и пятый классы;
- третья группа характеризуется ***мандатной*** защитой и содержит четвёртый, третий и второй классы;
- четвёртая группа характеризуется ***верифицированной*** защитой и содержит только первый класс.

Деление АС на соответствующие классы по условиям их функционирования с точки зрения защиты информации необходимо в целях разработки и применения обоснованных мер по достижению требуемого уровня защиты информации.

Дифференциация подхода к выбору методов и средств защиты определяется важностью обрабатываемой информации, различием АС по своему составу, структуре, способам обработки информации, количественному и качественному составу пользователей и обслуживающего персонала.

2. Утечка и несанкционированный доступ к информации

2.2. Несанкционированный доступ к информации

Основными этапами классификации АС являются:

- разработка и анализ исходных данных;
- выявление основных признаков АС, необходимых для классификации;
- сравнение выявленных признаков АС с классифицируемыми;
- присвоение АС соответствующего класса защиты информации от НСД.

Необходимыми исходными данными для проведения классификации конкретной АС являются:

- перечень защищаемых информационных ресурсов АС и их уровень конфиденциальности;
- перечень лиц, имеющих доступ к штатным средствам АС, с указанием их уровня полномочий;
- матрица доступа или полномочий субъектов доступа по отношению к защищаемым информационным ресурсам АС;
- режим обработки данных в АС.

Выбор класса АС производится заказчиком и разработчиком с привлечением специалистов по защите информации.

2. Утечка и несанкционированный доступ к информации

2.2. Несанкционированный доступ к информации

К числу определяющих признаков, по которым производится группировка АС в различные классы, относятся:

- наличие в АС информации различного уровня конфиденциальности;
- уровень полномочий субъектов доступа АС на доступ к конфиденциальной информации;
- режим обработки данных в АС - коллективный или индивидуальный.

Устанавливается девять классов защищённости АС от НСД к информации.

Каждый класс характеризуется определённой минимальной совокупностью требований по защите.

Классы подразделяются на три группы, отличающиеся особенностями обработки информации в АС.

В пределах каждой группы соблюдается иерархия требований по защите в зависимости от ценности (конфиденциальности) информации и, следовательно, иерархия классов защищённости АС.

2. Утечка и несанкционированный доступ к информации

2.2. Несанкционированный доступ к информации

Третья группа включает АС, в которых работает один пользователь, допущенный ко всей информации АС, размещённой на носителях одного уровня конфиденциальности. Группа содержит два класса – 3Б и 3А.

Вторая группа включает АС, в которых пользователи имеют одинаковые права доступа (полномочия) ко всей информации АС, обрабатываемой и (или) хранимой на носителях различного уровня конфиденциальности. Группа содержит два класса – 2Б и 2А.

Первая группа включает многопользовательские АС, в которых одновременно обрабатывается и (или) хранится информация разных уровней конфиденциальности. Не все пользователи имеют право доступа ко всей информации АС. Группа содержит пять классов – 1Д, 1Г, 1В, 1Б и 1А.

3. Подсистемы системы защиты информации

3.1. Требования к подсистемам системы защиты информации

Структура СЗИ состоит из комплекса подсистем, защищающих ИС организации на разных уровнях. Вне зависимости от вида деятельности и размера организации, базовыми подсистемами ИБ являются 4 подсистемы: управления доступом, регистрации и учёта, обеспечения целостности и криптографическая.

Создание СЗИ для конкретной организации в зависимости от класса защищённости, может потребовать разработки ряда дополнительных подсистем.

Ниже приведено описание требований к некоторым подсистемам СЗИ достаточно представительного класса защищённости – 1В.

Этому классу соответствует минимум требований, которым необходимо следовать, чтобы обеспечить конфиденциальность защищаемой информации.

Реальные АС часто не соответствуют данному классу.

3. Подсистемы системы защиты информации

3.1. Требования к подсистемам системы защиты информации

No п/п	Наименование подсистемы	Назначение
1	Управления доступом	Управление доступом к информационным ресурсам
2	Регистрации и учёта	Регистрация и учёт действий пользователей и процессов
3	Обеспечения целостности	Сохранение целостности и доступности информационных ресурсов
4	Криптографическая	Обеспечение конфиденциальности и аутентичности информации
5	Антивирусной защиты	Защита программ и данных от вирусов и вредоносных программ
6	Межсетевого экранирования	Контроль и фильтрации сетевых пакетов, защита сетей от НСД
7	Резервного копирования	Резервное копирование и восстановление информации
8	Обнаружения и предотвращения атак	Выявление и блокирование сетевых атак и подозрительных действий
9	Обеспечение отказоустойчивости	Обеспечение бесперебойной работы системы
10	Централизованного управления ИБ	Централизованный мониторинг и аудит событий

3. Подсистемы системы защиты информации

3.2. Подсистема управления доступом (идентификации и аутентификации пользователей)

Аутентификация – это процесс, в ходе которого на основании пароля, ключа или какой-либо иной информации, пользователь подтверждает, что является именно тем, за кого себя выдаёт.

Идентификация – это процесс, в ходе которого выясняются права доступа, привилегии, свойства и характеристики пользователя на основании его имени, логина или какой-либо другой информации о нём.

При входе пользователя в систему первым делом происходит его аутентификация. Если введённые пользователем логин и пароль совпадают с хранимыми в системе на сервере, то он успешно входит в систему, иначе ему отказывается в доступе.

При этом желательно контролировать количество попыток, чтобы избежать подбора паролей.

3. Подсистемы системы защиты информации

3.2. Подсистема управления доступом (идентификации и аутентификации пользователей)

Требования к функциям подсистемы управления доступом:

- должны осуществляться идентификация и проверка подлинности субъектов доступа при входе в систему по идентификатору (коду) и паролю условно-постоянного действия длиной не менее 6 буквенно-цифровых символов;
- должна осуществляться идентификация терминалов, ЭВМ, узлов сети ЭВМ, каналов связи, внешних устройств ЭВМ по их логическим адресам (номерам);
- должна осуществляться идентификация программ, томов, каталогов, файлов, записей, полей записей по именам;
- должно осуществляться управление потоками информации с помощью меток конфиденциальности. При этом уровень конфиденциальности накопителей должен быть не ниже уровня конфиденциальности записываемой на них информации.

3. Подсистемы системы защиты информации

3.3. Подсистема регистрации и учёта

Основные требования к подсистеме:

- должна осуществляться регистрация входа (выхода) субъектов доступа в систему (из системы), либо регистрация загрузки и инициализации операционной системы и её программного останова. Регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения АС. В параметрах регистрации указываются:
  - дата и время входа (выхода) субъекта доступа в систему (из системы) или загрузки (останова) системы;
  - результат попытки входа: успешная или неуспешная (при НСД);
  - идентификатор (код или фамилия) субъекта, предъявленный при попытке доступа;
- должна осуществляться регистрация выдачи печатных (графических) документов на "твёрдую" копию. Выдача должна сопровождаться автоматической маркировкой каждого листа (страницы) документа порядковым номером и учётными реквизитами АС с указанием на последнем листе документа общего количества листов (страниц);
- должна осуществляться регистрация запуска (завершения) программ и процессов (заданий, задач), предназначенных для обработки защищаемых файлов;
- должна осуществляться регистрация попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам;

3. Подсистемы системы защиты информации

3.3. Подсистема регистрации и учёта

- должна осуществляться регистрация попыток доступа ПС к следующим дополнительным защищаемым объектам доступа: терминалам, ЭВМ, узлам сети ЭВМ, линиям (каналам) связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей;
- должен осуществляться автоматический учёт создаваемых защищаемых файлов с помощью их дополнительной маркировки, используемой в подсистеме управления доступом. Маркировка должна отражать уровень конфиденциальности объекта;
- должен проводиться учёт всех защищаемых носителей информации с помощью их маркировки и с занесением учётных данных в журнал (учётную карточку);
- учёт защищаемых носителей должен проводиться в журнале (картотеке) с регистрацией их выдачи (приёма);
- должно проводиться несколько видов учёта (дублирующих) защищаемых носителей информации;
- должна осуществляться очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей. Очистка осуществляется двукратной произвольной записью в освобождаемую область памяти, ранее использованную для хранения защищаемых данных (файлов).

3. Подсистемы системы защиты информации

3.4. Подсистема обеспечения целостности

Основные требования к подсистеме:

- должна быть обеспечена целостность программных средств СЗИ НСД, обрабатываемой информации, а также неизменность программной среды. При этом:
  - целостность СЗИ НСД проверяется при загрузке системы по наличию имён (идентификаторов) компонент СЗИ;
  - целостность программной среды обеспечивается отсутствием в АС средств разработки и отладки программ;
- должны осуществляться физическая охрана СВТ (устройств и носителей информации), предусматривающая постоянное наличие охраны территории здания, где размещается АС, с помощью видеонаблюдения, использование строгого пропускного режима, специальное оборудование помещений АС;
- должен быть предусмотрен администратор (служба) ЗИ, ответственный за ведение, нормальное функционирование и контроль работы СЗИ НСД;
- должно проводиться периодическое тестирование функций СЗИ НСД при изменении программной среды и персонала АС с помощью тест – программ, имитирующих попытки НСД;

3. Подсистемы системы защиты информации

3.4. Подсистема обеспечения целостности

- должны быть в наличии средства восстановления СЗИ НСД, предусматривающие ведение двух копий программных средств СЗИ НСД, их периодическое обновление и контроль работоспособности;
- должны использоваться сертифицированные средства защиты. Их сертификацию проводят специальные сертификационные центры или специализированные предприятия, имеющие лицензию на проведение сертификации средств защиты СЗИ НСД.

3. Подсистемы системы защиты информации

3.5. Криптографическая подсистема

Криптографическая подсистема предназначена для обеспечения конфиденциальности (невозможности прочтения информации посторонним) и аутентичности (целостности и подлинности авторства, а также невозможности отказа от авторства) информации.

Основные требования к подсистеме:

- должно осуществляться шифрование всей конфиденциальной информации, записываемой на совместно используемые различными субъектами доступа (разделяемые) носители данных, в каналах связи, а также на съёмные носители данных (дискеты, микрокассеты и т.п.) долговременной внешней памяти для хранения за пределами сеансов работы санкционированных субъектов доступа. При этом должны выполняться автоматическое освобождение и очистка областей внешней памяти, содержавших ранее незашифрованную информацию;
- доступ субъектов к операциям шифрования и криптографическим ключам должен дополнительно контролироваться подсистемой управления доступом;
- должны использоваться сертифицированные средства криптографической защиты. Их сертификацию проводят специальные сертификационные центры или специализированные предприятия, имеющие лицензию на проведение сертификации криптографических средств защиты.

3. Подсистемы системы защиты информации

3.5. Криптографическая подсистема

При обмене электронными документами по сети возникает проблема аутентификации автора документа и самого документа, т.е. установления подлинности автора и отсутствия изменений в полученном документе. Для решения этой проблемы используется электронная цифровая подпись.

Электронная цифровая подпись (ЭЦП) – реквизит электронного документа, позволяющий установить отсутствие искажения информации в электронном документе с момента формирования ЭЦП и проверить принадлежность подписи владельцу сертификата ключа ЭЦП.

Электронная цифровая подпись предназначена для аутентификации лица, подписавшего электронный документ. Кроме этого, использование электронной цифровой подписи позволяет осуществить:

- доказательное подтверждение авторства документа;
- контроль целостности передаваемого документа: при любом случайном или преднамеренном изменении документа изменится подпись, следовательно, она станет недействительной;
- защиту от изменений (подделки) документа;
- невозможность отказа от авторства.

3. Подсистемы системы защиты информации

3.5. Криптографическая подсистема

ЭЦП формируется на основе самого документа и представляет собой относительно небольшое количество дополнительной информации, передаваемой вместе с подписываемым текстом.

Существует несколько схем построения цифровой подписи, например, на основе алгоритмов симметричного и асимметричного шифрования.

При формировании ЭЦП используются две процедуры:

1) процедуру постановки подписи;
2) процедуру проверки подписи.

Прежде всего, отправитель вычисляет хэш-функцию $h(M)$ подписываемого текста M. Вычисленное значение хэш-функции $h(M)$ представляет собой один короткий блок информации m, характеризующий весь текст M в целом.

Затем число m шифруется секретным ключом отправителя. Получаемая при этом пара чисел представляет собой ЭЦП для данного текста M.

3. Подсистемы системы защиты информации

3.5. Криптографическая подсистема

Хэш-функция (англ. *hash* – мелко измельчать и перемешивать) предназначена для сжатия подписываемого документа до нескольких десятков или сотен бит. Значение хэш-функции $h(M)$ сложным образом зависит от документа M и не позволяет восстановить сам документ M.

При проверке ЭЦП получатель сообщения снова вычисляет хэш-функцию $m = h(M)$ принятого по каналу текста M, после чего при помощи открытого ключа отправителя проверяет, соответствует ли полученная подпись вычисленному значению m хэш-функции.

3. Подсистемы системы защиты информации

3.6. Подсистема антивирусной защиты

В соответствии с ГОСТ Р 51188–98 – Защита информации. Испытание программных средств на наличие компьютерных вирусов эта подсистема должна отвечать следующим требованиям:

- организация мониторинга антивирусной активности;
- создание двухуровневой антивирусной защиты с применением антивирусного ПО различных производителей;
- обеспечение антивирусной защиты серверного оборудования.

Компьютерный вирус – специально написанная небольшая программа, которая может сама присоединяться к другим программам для выполнения каких-либо вредоносных действий. Компьютерный вирус был назван по аналогии с биологическими вирусами за сходный механизм распространения.

Самые распространённые каналы заражения: дискеты, флеш-накопители, электронная почта, системы обмена мгновенными сообщениями, веб-страницы, Интернет и локальные сети.

3. Подсистемы системы защиты информации

3.6. Подсистема антивирусной защиты

Вирусы принято разделять:

1) по среде обитания – загрузочные, файловые, файлово-загрузочные, сетевые;
2) по степени воздействия – безвредные, неопасные, опасные, разрушительные;
3) по способам заражения: резидентные, нерезидентные;
4) по алгоритмическим особенностям – репликаторы (черви), троянский конь, логическая бомба, мутанты, стелс-вирусы (невидимки), макровирусы.

В настоящее время существует большое разнообразие антивирусных программ:

- программы-детекторы могут находить только известные им вирусы (AidsTest Д. Н. Лозинского, Dr. Web А.И. Данилова);
- программы-доктора или фаги, а также программы-вакцины не только находят заражённые файлы, но и удаляют из файла тело программы-вируса. Среди фагов выделяют полифаги, предназначенные для поиска и уничтожения большого количества вирусов (AVP, Aidstest, Scan, Norton AntiVirus, Doctor Web);
- программы-ревизоры. Самое надёжное средство защиты от вирусов. Ревизоры запоминают исходное состояние программ, каталогов и системных областей диска, а затем периодически сравнивают текущее состояние с исходным. Обнаруженные изменения выводятся на видеомонитор (ADinf, ADinf32);

3. Подсистемы системы защиты информации

3.6. Подсистема антивирусной защиты

- программы-фильтры или «сторожа» – небольшие резидентные программы, предназначенные для обнаружения подозрительных действий при работе компьютера (AVP, Norton Antivirus, McAfee Virus Scan 95);
- антивирусные комплексы, выполняющие обнаружение, лечение, блокирование, восстановление, регистрацию, обеспечение целостности, обновление базы данных компьютерных вирусов (Norton Antivirus, пакет AVR (AntiViral Toolkit Pro) –лаборатории Е. Касперского).

Выделяют также следующие разновидности антивирусных программ:

- антивирусные сканеры – пионеры антивирусного движения, которые ищут в файлах, памяти, и загрузочных секторах вирусные маски (описания) известных вирусов, хранящиеся в специальной базе данных. Проверка файлов производится только по инициативе пользователя после запуска программ;
- антивирусные мониторы (файловые, для почтовых программ, для специальных приложений) – осуществляют автоматическую проверку всех используемых файлов в масштабе реального времени. В случае обнаружения вредоносной программы, монитор, в зависимости от настроек, вылечит файл, заблокирует его выполнение или изолирует, переместив в специальную карантинную директорию для дальнейшего исследования;
- программа-брандмауэр, предназначенная для защиты компьютера от

3. Подсистемы системы защиты информации

3.6. Подсистема антивирусной защиты

Рекомендации по профилактике заражения:

- проверять на наличие вирусов все поступающие извне данные;
- периодически проверять все жёсткие диски ПК на наличие вирусов;
- использовать лицензионные программные продукты;
- ограничить доступ к ПК других пользователей;
- защищать свои гибкие диски от записи при работе на других ПК;
- не оставлять в кармане дисковода дискету при включении или перезагрузке ПК, чтобы исключить заражение ПК загрузочными вирусами;
- регулярно обновлять антивирусные программы.

3. Подсистемы системы защиты информации

3.7. Подсистема межсетевого экранирования

Межсетевой экран (МЭ) или сетевой экран – комплекс аппаратных или программных средств, осуществляющий контроль и фильтрацию проходящих через него сетевых пакетов в соответствии с заданными правилами.

Основной задачей сетевого экрана является защита компьютерных сетей или отдельных узлов от несанкционированного доступа. Кроме того, МЭ позволяют разделить сеть на две или более частей и реализовать набор правил, определяющих условия прохождения сетевых пакетов из одной части в другую.

Некоторые сетевые экраны позволяют осуществлять трансляцию адресов – динамическую замену внутрисетевых адресов или портов на внешние, используемые за пределами ЛВС.

Сетевые экраны часто называют фильтрами, так как их основная задача – не пропускать (фильтровать) пакеты, не подходящие под критерии, определённые в конфигурации. Фильтрация может осуществляться на любом уровне модели OSI. В качестве критериев может выступать информация с разных уровней: адреса отправителя/получателя, номера портов, содержимое поля данных.

3. Подсистемы системы защиты информации

3.7. Подсистема межсетевого экранирования

Эквивалентными термину межсетевой экран являются названия:

- брандмауэр (нем. *Brandmauer*) – стена из огнеупорного материала, воздвигаемая на пути распространения пожара;
- файерволл (англ. Firewall) – горящая стена (fire – огонь, wall – стена).

Модель OSI (Open System Interconnection reference model) или модель взаимодействия открытых систем – это многоуровневая система, отражающая взаимодействие программного и аппаратного обеспечения при осуществлении сеанса связи в сети.

В модели OSI сетевые функции распределены между 7 уровнями.

Каждому уровню соответствуют различные сетевые операции, оборудование и протоколы. Каждый уровень поддерживает интерфейсы с выше- и нижележащими уровнями.

Различают следующие уровни (сверху вниз):

1) прикладной;
2) представления;
3) сеансовый;
4) транспортный;
5) сетевой;
6) канальный;
7) физический.

3. Подсистемы системы защиты информации

3.7. Подсистема межсетевого экранирования

Безопасное межсетевое взаимодействие для информационных систем достигается путём применения средств межсетевого экранирования (межсетевых экранов), которые обеспечивают в соответствии с приказом 58 ФСТЭК:

- фильтрацию на сетевом уровне для каждого сетевого пакета независимо (решение о фильтрации принимается на основе сетевых адресов отправителя и получателя или на основе других эквивалентных атрибутов);
- идентификацию и аутентификацию администратора МЭ при его локальных запросах на доступ по идентификатору (коду) и паролю условно-постоянного действия;
- регистрацию входа (выхода) администратора МЭ в систему (из системы) либо загрузки и инициализации системы и её программного останова (регистрация выхода из системы не проводится в моменты аппаратурного отключения МЭ);
- контроль целостности своей программной и информационной части;
- фильтрацию пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств;
- восстановление свойств МЭ после сбоев и отказов оборудования;
- регламентное тестирование реализации правил фильтрации, процесса идентификации и аутентификации администратора МЭ, процесса регистрации действий администратора МЭ, процесса контроля за целостностью программной и информационной части, процедуры

3. Подсистемы системы защиты информации

3.8. Подсистема резервного копирования и архивирования

Подсистемы резервного копирования – это программно-аппаратные комплексы, предназначенные для:

- проведения регулярного автоматического копирования, как системных данных, так и данных, создаваемых пользователями, на специально предназначенные для этого накопители;
- оперативного восстановления данных (в случае утери или по каким-то другим причинам).

Подсистема должна соответствовать следующим требованиям:

- поддержка всех основных сетевых и клиентских ОС;
- наличие документов и инструкций, регламентирующих процесс резервного копирования и архивирования в соответствии с производственной необходимостью;
- ведение подробных журналов выполняемых операций и сообщений;
- организация резервного копирования для всех серверов, указанных в регламентах резервного копирования;
- разработка процедуры и регулярное проведение тестирования резервных копий.
- простота использования.

3. Подсистемы системы защиты информации

3.9. Подсистема обнаружения атак

Подсистема обнаружения атак предназначена для своевременного обнаружения и предотвращения атак на узлы сети.

В функции подсистемы входит:

- обнаружение враждебной деятельности и распознавание атак на узлы сети;
- захват сетевого трафика;
- обработка сетевого трафика на основе заданной политики и имеющейся базы данных сигнатур атак. Сигнатура атаки (вируса) – характерные признаки атаки или вируса, используемые для их обнаружения. Наряду с сигнатурными методами необходимо использовать и поведенческие методы анализа информации. Поведенческие методы используется для выявления атак на основе обнаружения отклонений от штатного поведения ИС. Наиболее часто поведенческий метод реализуется на основе статистических моделей;
- блокирование сетевых атак посредством фильтрации потенциально опасных пакетов данных;
- использование методов активного и пассивного реагирования. Пассивное реагирование предполагает оповещение администратора о выявленной атаке, активное – блокирование попытки реализации атаки.

Серьёзной проблемой при разработке подсистемы обнаружения атак является борьба с ложными срабатываниями (false positive).

3. Подсистемы системы защиты информации

3.10. Подсистема обеспечения отказоустойчивости

Отказоустойчивость (fault tolerance) – это способность системы сохранять работоспособность при отказах отдельных устройств, блоков, схем. В отказоустойчивой системе отказ одного из её элементов приводит к некоторому снижению качества её работы (деградации), а не к полному останову.

С понятием отказоустойчивости тесно связаны вопросы надёжности СЗИ.

Применительно к СЗИ от НСД ***надёжность*** – это свойство системы защиты обеспечивать защиту информации от НСД в течение заданного промежутка времени.

Подсистема обеспечения отказоустойчивости должна обеспечивать бесперебойную работу:

- внешних дисковых подсистем в случае выхода из строя жёсткого диска;
- серверов;
- АРМ пользователей.

3. Подсистемы системы защиты информации

3.11. Подсистема централизованного управления ИБ

Управление – это совокупность целенаправленных действий, включающих в себя оценку ситуации и состояния объектов управления, выбор управляющих воздействий и их реализацию (планирование и внедрение мер обеспечения безопасности).

Эффективность СЗИ во многом зависит от наличия в её составе средств, обеспечивающих сбор, анализ, хранение информации о состоянии системы ИБ, а также централизованного управления всеми её составляющими.

Вся система в целом, как и каждая из её подсистем, должны соответствовать общей политике безопасности. Для отслеживания работоспособности отдельных подсистем, организации мониторинга, определения и своевременного реагирования на угрозы ИБ и других событий предназначена подсистема централизованного управления компонентами системы, выполняющая следующие функции:

- мониторинг и аудит данных о событиях безопасности;
- оперативное оповещение об инцидентах безопасности;
- генерацию сводных отчётов с рекомендациями по управлению ИБ.

Кроме того, распределённая атака на ИС в некоторых случаях может быть зафиксирована и предотвращена только при получении данных из многих точек сети, как от средств защиты, так и от серверов, сетевого оборудования, приложений. Зафиксировать такую атаку можно, имея средства консолидации