Типы угроз безопасности ПДн

Угрозы безопасности ПДн классифицируются по типу используемой уязвимости ИСПДн. Выделяются следующие типы угроз:

 угрозы, связанные с наличием недокументированных (не декларированных) возможностей в системном программном обеспечении, используемом в ИСПДн (угрозы 1-го типа);

 угрозы, связанные с наличием недокументированных (не декларированных) возможностей в прикладном программном обеспечении, используемом в ИСПДн (угрозы 2-го типа);

* угрозы, не связанные с наличием недокументированных (не декларированных) возможностей в системном и прикладном программном обеспечении, используемом в ИСПДн (угрозы 3-го типа).

Угрозы утечки информации по техническим каналам

При обработке ПДн в ИСПДн возможно возникновение угроз безопасности ПДн за счет реализации следующих технических каналов утечки информации:

1. Угрозы утечки акустической (речевой) информации.
2. Угрозы утечки видовой информации.
3. Угрозы утечки информации по каналам ПЭМИН.

Угрозы утечки акустической (речевой) информации

Возникновение угроз утечки акустической (речевой) информации, содержащейся непосредственно в произносимой речи пользователя ИСПДн, при обработке ПДн в ИСПДн, возможно при наличии функций голосового ввода ПДн

* ИСПДн или функций воспроизведения ПДн акустическими средствами ИСПДн. Утечка акустической (речевой) информации может быть осуществлена:
  + с помощью аппаратных закладок;
  + за счет съема виброакустических сигналов;
  + за счет излучений, модулированных акустическим сигналом (микрофонный эффект и ВЧ облучение);
  + за счет оптического излучения, модулированного акустическим

сигналом.

Угрозы утечки видовой информации

Угрозы утечки видовой информации реализуются за счет просмотра ПДн с помощью оптических (оптикоэлектронных) средств с экранов дисплеев и других средств отображения средств вычислительной техники, информационно-

вычислительных комплексов, технических средств обработки графической, видео

* и буквенно-цифровой информации, входящих в состав ИСПДн.

Кроме этого, просмотр (регистрация) ПДн возможен с использованием специальных электронных устройств съема, внедренных в служебных помещениях или скрытно используемых физическими лицами при посещении ими служебных помещений.

Необходимым условием осуществления просмотра (регистрации) ПДн является наличие прямой видимости между средством наблюдения и носителем ПДн.

Утечка видовой информации может быть осуществлена:

* за счет удаленного просмотра экранов дисплеев и других средств отображения информации,
* с помощью видео аппаратных закладок.

Угрозы утечки информации по каналам ПЭМИН

Возникновение угрозы ПДн по каналам ПЭМИН возможно за счет перехвата техническими средствами побочных (не связанных с прямым

функциональным значением элементов ИСПДн) информативных электромагнитных полей и электрических сигналов, возникающих при обработке ПДн техническими средствами ИСПДн.

Генерация информации, содержащей ПДн и циркулирующей в технических средствах ИСПДн в виде электрических информативных сигналов, обработка и передача указанных сигналов в электрических цепях технических средств ИСПДн сопровождается побочными электромагнитными излучениями, которые могут распространяться за пределы служебных помещений в зависимости от мощности излучений и размеров ИСПДн.

Регистрация ПЭМИН осуществляется с целью перехвата информации, циркулирующей в технических средствах, осуществляющих обработку ПДн

(средствах вычислительной техники, информационно-вычислительных комплексах и сетях, средствах и системах передачи, приема и обработки ПДн, средствах и системах звукозаписи, звукоусиления, звуковоспроизведения, переговорных и телевизионных устройствах, средствах изготовления, тиражирования документов и других технических средствах обработки речевой, графической, видео - и буквенно-цифровой информации).

Для регистрации ПЭМИН используется аппаратура в составе радиоприемных устройств и оконечных устройств восстановления информации.

Утечка информации по каналам ПЭМИН может быть осуществлена:

* за счет побочных электромагнитных излучений электронно-вычислительной техники;
* за счет наводок по цепям питания;
* за счет радиоизлучений, модулированных информационным

сигналом.

Угрозы НСД

Угрозы НСД в ИСПДн с применением программных и программно-аппаратных средств реализуются при осуществлении несанкционированного, в том числе случайного доступа, в результате которого осуществляется нарушение конфиденциальности (копирование, несанкционированное распространение), целостности (уничтожение, изменение) и доступности (блокирование) ПДн, и включают в себя:

* 1. Угрозы НСД, связанные с действиями нарушителей, имеющих доступ
* ИСПДн.
  1. Угрозы, связанные с реализацией протоколов сетевого взаимодействия, реализуемые внутри распределенной сети.
  2. Угрозы внедрения (в том числе по сети) вредоносных программ (программно-математического воздействия).

Угрозы НСД, связанные с действиями нарушителей, имеющих доступ к ИСПДн.

Данные угрозы могут быть реализованы нарушителем в случае получения физического доступа к ИСПДн или, по крайней мере, к средствам ввода информации в ИСПДн. При этом можно выделить следующие угрозы:

1. Угрозы, реализуемые в ходе загрузки операционной системы.

Эти угрозы безопасности информации направлены на перехват паролей или идентификаторов, модификацию программного обеспечения базовой системы ввода-вывода (BIOS), перехват управления загрузкой с изменением необходимой технологической информации для получения НСД в операционную среду ИСПДн. Чаще всего такие угрозы реализуются с использованием отчуждаемых носителей информации.

1. Угрозы, реализуемые после загрузки операционной среды, независимо от того, какая прикладная программа запускается пользователем.

Эти угрозы, как правило, направлены на выполнение непосредственно несанкционированного доступа к информации. При получении доступа в операционную среду нарушитель может воспользоваться как стандартными функциями операционной системы (уничтожение, копирование, перемещение, форматирование носителей информации и т.п.) или какой-либо прикладной программой общего пользования (например, системы управления базами данных), так и специально созданными для выполнения несанкционированного доступа программами, например:

* + программами просмотра и модификации реестра;
  + программами поиска текстов в текстовых файлах по ключевым словам
* копирования;
  + специальными программами просмотра и копирования записей в базах

данных;

-- программами быстрого просмотра графических файлов, их редактирования или копирования;

* программами поддержки возможностей реконфигурации программной среды (настройки ИСПДн в интересах нарушителя) и др.
* Кроме того, к данным угрозам необходимо отнести угрозы утечки информации путем копирования ее на съемные носители.

1. Угрозы, реализуемые после загрузки операционной среды, реализация которых определяется тем, какая из прикладных программ запускается пользователем, или фактом запуска любой из прикладных программ. Большая часть таких угроз представляет собой угрозы внедрения вредоносных программ.

Угрозы, связанные с реализацией протоколов сетевого взаимодействия, реализуемые внутри распределенной сети

Можно выделить следующие угрозы, реализуемые с использованием протоколов сетевого взаимодействия, реализуемые внутри распределенной сети:

1. Угрозы «Анализа сетевого трафика».

Эта угроза реализуется с помощью специальной программы-анализатора пакетов (sniffer), перехватывающей все пакеты, передаваемые по сегменту сети, и выделяющей среди них те, в которых передаются идентификатор пользователя и его пароль, а также конфиденциальная информация.

1. Угрозы сканирования сети.

Сущность процесса реализации угрозы заключается в передаче запросов сетевым службам хостов ИСПДн и анализе ответов от них с целью выявления используемых протоколов, доступных портов сетевых служб, законов формирования идентификаторов соединений, определение активных сетевых сервисов, подбора идентификаторов и паролей пользователей.

1. Угрозы выявления паролей.

Цель реализации угрозы состоит в получении НСД путем преодоления парольной защиты. Злоумышленник может реализовывать угрозу с помощью целого ряда методов, таких как простой перебор, перебор с использованием специальных словарей, установка вредоносной программы для перехвата пароля, подмена доверенного объекта сети (IP-spoofing) и перехват пакетов (sniffing). В основном для реализации угрозы используются специальные программы, которые пытаются получить доступ к хосту путем последовательного подбора паролей. В случае успеха злоумышленник может создать для себя «проход» для будущего доступа, который будет действовать, даже если на хосте изменить пароль доступа.

1. Угрозы навязывания ложного маршрута сети.

Данная угроза реализуется путем несанкционированного изменения маршрутно-адресных данных. Возможность навязывания ложного маршрута обусловлена недостатками, присущими алгоритмам маршрутизации (в частности, из-за проблемы идентификации сетевых управляющих устройств), в результате

чего можно попасть, например, на хост или в сеть злоумышленника, где можно войти в операционную среду технического средства в составе ИСПДн. Реализация угрозы основывается на несанкционированном использовании протоколов маршрутизации (RIP, OSPF, LSP) и управления сетью (ICMP, SNMP) для внесения изменений в маршрутно-адресные таблицы. При этом нарушителю необходимо послать от имени сетевого управляющего устройства (например, маршрутизатора) управляющее сообщение.

1. Угрозы внедрения ложного объекта сети.

Эта угроза основана на использовании недостатков алгоритмов удаленного поиска. В случае если объекты сети изначально не имеют адресной информации друг о друге, используются различные протоколы удаленного поиска (например, SAP в сетях Novell NetWare; ARP, DNS, WINS в сетях со стеком протоколов TCP/IP), заключающиеся в передаче по сети специальных запросов и получении на них ответов с искомой информацией. При этом существует возможность перехвата нарушителем поискового запроса и выдачи на него ложного ответа, использование которого приведет к требуемому изменению маршрутно-адресных данных. В дальнейшем весь поток информации, ассоциированный с объектом-жертвой, будет проходить через ложный объект сети.

1. Угрозы типа «Отказ в обслуживании».

Эти угрозы основаны на недостатках сетевого программного обеспечения, его уязвимостях, позволяющих нарушителю создавать условия, когда операционная система оказывается не в состоянии обрабатывать поступающие пакеты.

Может быть выделено несколько разновидностей таких угроз:

* скрытый отказ в обслуживании, вызванный привлечением части ресурсов ИСПДн на обработку пакетов, передаваемых злоумышленником со снижением пропускной способности каналов связи, производительности сетевых устройств, нарушением требований к времени обработки запросов. Примерами реализации угроз подобного рода могут служить: направленный шторм эхо-запросов по протоколу ICMP (Pingflooding), шторм запросов на установление TCP-соединений (SYN-flooding), шторм запросов к FTP-серверу;
* явный отказ в обслуживании, вызванный полным исчерпанием ресурсов ИСПДн при обработке пакетов, передаваемых злоумышленником (занятие всей полосы пропускания каналов связи, переполнение очередей запросов на обслуживание), при котором легальные запросы не могут быть переданы через сеть из-за недоступности среды передачи либо получают отказ в обслуживании ввиду переполнения очередей запросов, дискового пространства памяти и т.д. Примерами угроз данного типа могут служить шторм широковещательных ICMP-эхо-запросов (Smurf), направленный шторм (SYN-

flooding), шторм сообщений почтовому серверу (Spam); явный отказ в обслуживании, вызванный нарушением логической связности между техническими средствами ИСПДн при передаче нарушителем

управляющих сообщений от имени сетевых устройств, приводящих к изменению маршрутно-адресных данных (например, ICMP Redirect Host, DNS-flooding) или

идентификационной и аутентификационной информации; явный отказ в обслуживании, вызванный передачей злоумышленником пакетов с нестандартными атрибутами (угрозы типа «Land», «Tear Drop», «Bonk», «Nuke», «UDP-bomb») или имеющих длину, превышающую максимально допустимый размер (угроза типа «Ping Death»), что может привести к сбою сетевых устройств, участвующих в обработке запросов, при условии наличия ошибок в программах, реализующих протоколы сетевого обмена.

Результатом реализации данной угрозы может стать нарушение работоспособности соответствующей службы предоставления удаленного доступа

* ПДн в ИСПДн, передача с одного адреса такого количества запросов на подключение к техническому средству в составе ИСПДн, какое максимально может «вместить» трафик (направленный «шторм запросов»), что влечет за собой переполнение очереди запросов и отказ одной из сетевых служб или полная остановка ИСПДн из-за невозможности системы заниматься ничем другим, кроме обработки запросов;
  1. Угрозы удаленного запуска приложений.

Угроза заключается в стремлении запустить на хосте ИСПДн различные предварительно внедренные вредоносные программы:

* программы-закладки;
* вирусы;
* «сетевые шпионы» и т.д.

Основная цель внедренных вредоносных программ – нарушение конфиденциальности, целостности, доступности информации и полный контроль за работой хоста. Кроме того, возможен несанкционированный запуск прикладных программ пользователей для несанкционированного получения необходимых нарушителю данных, для запуска управляемых прикладной программой процессов и др.

Выделяют три подкласса данной угрозы:

a) распространение файлов, содержащих несанкционированный исполняемый код. Типовые угрозы этого подкласса основываются на активизации распространяемых файлов при случайном обращении к ним. Примерами таких файлов могут служить: файлы, содержащие исполняемый код в виде макрокоманд (документы Microsoft Word, Excel и т.п.); html-документы, содержащие исполняемый код в виде элементов ActiveX, Java-апплетов, интерпретируемых скриптов (например, тексты на JavaScript); файлы, содержащие исполняемые коды программ. Для распространения файлов могут использоваться службы электронной почты, передачи файлов, сетевой файловой системы;

1. удаленный запуск приложения путем переполнения буфера приложений-серверов. При угрозах этого подкласса используются недостатки программ, реализующих сетевые сервисы (в частности, отсутствие контроля за

переполнением буфера). Настройкой системных регистров иногда удается переключить процессор после прерывания, вызванного переполнением буфера, на исполнение кода, содержащегося за границей буфера. Примером реализации такой угрозы может служить внедрение широко известного «вируса Морриса»;

1. удаленный запуск приложения путем использования возможностей удаленного управления системой, предоставляемых скрытыми программными и аппаратными закладками, либо используемыми штатными средствами. При угрозах этого подкласса нарушитель использует возможности удаленного управления системой, предоставляемые скрытыми компонентами (например, «троянскими» программами типа BackOrifice, NetBus), либо штатными средствами управления и администрирования компьютерных сетей (Landesk Management Suite, Managewise, BackOrifice и т. п.). В результате их использования удается добиться удаленного контроля над станцией в сети.

Угрозы внедрения по сети вредоносных программ (программно-математического воздействия)

Программно-математическое воздействие - это воздействие с помощью вредоносных программ. Программой с потенциально опасными последствиями или вредоносной программой называют некоторую самостоятельную программу (набор инструкций), которая способна выполнять любое непустое подмножество следующих функций:

* скрывать признаки своего присутствия в программной среде компьютера;
* обладать способностью к самодублированию, ассоциированию себя с другими программами и (или) переносу своих фрагментов в иные области оперативной или внешней памяти;
* разрушать (искажать произвольным образом) код программ в оперативной памяти;
* выполнять без инициирования со стороны пользователя (пользовательской программы в штатном режиме ее выполнения) деструктивные функции (копирования, уничтожения, блокирования и т.п.);
  + сохранять фрагменты информации из оперативной памяти в некоторых областях внешней памяти прямого доступа (локальных или удаленных);
* искажать произвольным образом, блокировать и (или) подменять выводимый во внешнюю память или в канал связи массив информации, образовавшийся в результате работы прикладных программ, или уже находящиеся во внешней памяти массивы данных.

Вредоносные программы могут быть внесены (внедрены) как преднамеренно, так и случайно в программное обеспечение, используемое в ИСПДн, в процессе его разработки, сопровождения, модификации и настройки. Кроме этого, вредоносные программы могут быть внесены в процессе эксплуатации ИСПДн с внешних носителей информации или посредством

сетевого взаимодействия как в результате НСД, так и случайно пользователями ИСПДн.

Вредоносные программы основаны на использовании уязвимостей различного рода программного обеспечения и разнообразных сетевых технологий, обладают широким спектром возможностей и могут действовать во всех видах программного обеспечения.

Наличие в ИСПДн вредоносных программ может способствовать возникновению скрытых, в том числе нетрадиционных каналов доступа к информации, позволяющих вскрывать, обходить или блокировать защитные механизмы, предусмотренные в системе, в том числе парольную защиту.

Источники угроз безопасности ПДн

Источник угрозы безопасности информации – субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации.

Источниками угроз НСД в ИСПДн могут быть:

* нарушитель;
* носитель вредоносной программы;
* аппаратная закладка.

Категории нарушителей безопасности ПДн

Целью возможного нарушителя является нарушение характеристик безопасности защищаемых объектов путем модификации, разрушения или блокирования программных и технических средств, хищения и ознакомления с защищаемой информацией, а также навязывания ложной информации, или побуждения к принятию неверных решений.

Контролируемой зоной является:

-- территория офиса, включая помещения общего доступа, предназначенные для работы с клиентами;

* серверное помещение, расположенное в Институте.



Рабочие станции пользователей, расположенные в помещениях общего доступа, находятся под постоянным визуальным наблюдением работников Института, в связи с этим доступ посторонних лиц к рабочим стациям ограничен.

* точки зрения наличия возможности постоянного или разового доступа в контролируемую зону, в которой размещены технические средства ИСПДн, все нарушители могут быть отнесены к следующим двум категориям:

-- категория I: внешние нарушители - физические лица, не имеющие права пребывания на территории контролируемой зоны, в пределах которой размещаются технические средства ИСПДн Института, а также права легального физического доступа к техническим средствам ИСПДн;

-- категория II: внутренние нарушители - физические лица, имеющие право пребывания на территории контролируемой зоны, в пределах которой размещаются технические средства ИСПДн Института.

Под внешним нарушителем информационной безопасности рассматривается нарушитель, не имеющий непосредственного доступа к техническим средствам и ресурсам системы, находящимся в пределах контролируемой зоны.