Приложение №1
к приказу №97 от 11.09.2026

Государственное бюджетное учреждение
Ивановской области «Ивановский государственный театральный комплекс»

Утверждаю
Директор ГБУ «ИГТК»,
_____, Соколов С.Н.
«11» 09 202 6 года
М. П.

Модель угроз и нарушителя безопасности персональных данных, обрабатываемых в информационных системах, используемых в Государственном бюджетном учреждении Ивановской области «Ивановский государственный театральный комплекс» (ГБУ «ИГТК»)

Обозначения и сокращения
АРМ – автоматизированное рабочее место
ВИ – видовая информация
ВТСС – вспомогательные технические средства и системы
ИСПДн – информационная система персональных данных
КЗ – контролируемая зона
МЭ – межсетевой экран
НДВ – недекларированные возможности
НСД – несанкционированный доступ
ОБПДн – обеспечение безопасности персональных данных
ОС – операционная система
ПДн – персональные данные
ПМВ – программно-математическое воздействие
ПО – программное обеспечение
ПЭМИН – побочные электромагнитные излучения и наводки
РИ – речевая информация
СВТ – средство вычислительной техники
СЗИ – средство защиты информации
СПИ – стеганографическое преобразование информации
СЭУПИ – специальные электронные устройства перехвата информации
ТКУИ – технический канал утечки информации
ТСОИ – технические средства обработки информации
УБПДн – угрозы безопасности персональных данных

1. Термины и определения

В настоящем документе используются следующие термины и их определения:

Автоматизированная система - система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

Аутентификация отправителя данных - подтверждение того, что отправитель полученных данных соответствует заявленному.

Безопасность персональных данных - состояние защищенности персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность

персональных данных при их обработке в информационных системах персональных данных.

Блокирование персональных данных - временное прекращение сбора, систематизации, накопления, использования, распространения, персональных данных, в том числе их передачи.

Вирус (компьютерный, программный) - исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению.

Вредоносная программа - программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных.

Вспомогательные технические средства и системы - технические средства и системы, не предназначенные для передачи, обработки и хранения персональных данных, устанавливаемые совместно с техническими средствами и системами, предназначенными для обработки персональных данных, или в помещениях, в которых установлены информационные системы персональных данных.

Доступ в операционную среду компьютера (информационной системы персональных данных) - получение возможности запуска на выполнение штатных команд, функций, процедур операционной системы (уничтожения, копирования, перемещения и т.п.), исполняемых файлов прикладных программ.

Доступ к информации - возможность получения информации и ее использования.

Закладочное устройство - элемент средства съема информации, скрытно внедряемый (закладываемый или вносимый) в места возможного съема информации (в том числе в ограждение, конструкцию, оборудование, предметы интерьера, транспортные средства, а также в технические средства и системы обработки информации).

Защищаемая информация - информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Идентификация - присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Информативный сигнал - электрические сигналы, акустические, электромагнитные и другие физические поля, по параметрам которых может быть раскрыта конфиденциальная информация (персональные данные), обрабатываемая в информационной системе персональных данных.

Информационная система персональных данных – это информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

Информационные технологии - процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

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

Контролируемая зона – это пространство, в котором исключено неконтролируемое пребывание сотрудников и посетителей оператора и посторонних транспортных, технических и иных материальных средств.

Конфиденциальность персональных данных - обязательное для соблюдения

оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания.

Межсетевой экран - локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в информационную систему персональных данных и (или) выходящей из информационной системы.

Нарушитель безопасности персональных данных - физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности персональных данных при их обработке техническими средствами в информационных системах персональных данных.

Недекларированные возможности - функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

Несанкционированный доступ (несанкционированные действия) - доступ к информации или действия с информацией, осуществляемые с нарушением установленных прав и (или) правил доступа к информации или действий с ней с применением штатных средств информационной системы или средств, аналогичных им по своим функциональному предназначению и техническим характеристикам.

Носитель информации - физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

Обработка персональных данных - действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

Оператор - государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

Перехват (информации) - неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов.

Персональные данные - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

Побочные электромагнитные излучения и наводки - электромагнитные излучения технических средств обработки защищаемой информации, возникающие как побочное явление и вызванные электрическими сигналами, действующими в их электрических и магнитных цепях, а также электромагнитные наводки этих сигналов на токопроводящие линии, конструкции и цепи питания.

Пользователь информационной системы персональных данных - лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования.

Правила разграничения доступа - совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

Программная закладка - скрытно внесенный в программное обеспечение функциональный объект, который при определенных условиях способен обеспечить несанкционированное программное воздействие. Программная закладка может быть реализована в виде

вредоносной программы или программного кода.

Программное (программно-математическое) воздействие - несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ.

Ресурс информационной системы - именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы.

Средства вычислительной техники - совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

Субъект доступа (субъект) - лицо или процесс, действия которого регламентируются правилами разграничения доступа.

Технические средства информационной системы персональных данных - средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки персональных данных (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации.

Технический канал утечки информации - совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.

Угрозы безопасности персональных данных - совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.

Уничтожение персональных данных - действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.

Утечка (защищаемой) информации по техническим каналам - неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

Уязвимость - некая слабость, которую можно использовать для нарушения системы или содержащейся в ней информации.

Целостность информации - состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право.

2. Общие положения

Настоящая «Модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных, используемых в ГБУ «ИГТК»» (далее – Модель угроз) содержит систематизированный перечень угроз безопасности персональных данных при их обработке в информационных системах персональных данных, используемых в ГБУ «ИГТК». Эти угрозы обусловлены преднамеренными или непреднамеренными действиями физических лиц, действиями зарубежных спецслужб или организаций (в том числе террористических), а также криминальных группировок, создающих условия (предпосылки) для нарушения безопасности персональных данных (ПДн), которое ведет к ущербу жизненно важных интересов личности, общества и государства.

Модель угроз содержит единые исходные данные по угрозам безопасности

персональных данных, обрабатываемых в информационных системах персональных данных (ИСПДн), связанным:

- с перехватом (съемом) ПДн по техническим каналам с целью их копирования или неправомерного распространения;
- с несанкционированным, в том числе случайным, доступом в ИСПДн с целью изменения, копирования, неправомерного распространения ПДн или деструктивных воздействий на элементы ИСПДн и обрабатываемых в них ПДн с использованием программных и программно-аппаратных средств с целью уничтожения или блокирования ПДн.

Модель угроз является методическим документом, используемым в ГБУ «ИГТК», которое является оператором ПДН, самостоятельно обрабатывающим ПДНв ИСПДН. С применением Модели угроз решаются следующие задачи:

- анализ защищенности ИСПДн от угроз безопасности ПДн в ходе организации и выполнения работ по обеспечению безопасности ПДн;
- разработка системы защиты ПДн, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты ПДн, предусмотренных для соответствующего класса ИСПДн;
- проведение мероприятий, направленных на предотвращение несанкционированного доступа к ПДн и (или) передачи их лицам, не имеющим права доступа к такой информации;
- недопущение воздействия на технические средства ИСПДн, в результате которого может быть нарушено их функционирование;
- контроль обеспечения уровня защищенности персональных данных.

В Модели угроз дано обобщенное описание ИСПДн как объектов защиты, возможных источников угрозы безопасности персональных данных (УБПДн), основных классов уязвимостей ИСПДн, возможных видов деструктивных воздействий на ПДн, а также основных способов их реализации.

Угрозы безопасности ПДн, обрабатываемых в ИСПДн, содержащиеся в настоящей Модели угроз, могут уточняться и дополняться по мере выявления новых источников угроз, развития способов и средств реализации УБПДн в ИСПДн. Внесение изменений в Модель угроз осуществляется ГБУ «ИГТК» в устанавливаемом порядке.

3. Классификация угроз безопасности персональных данных

Состав и содержание УБПДн определяется совокупностью условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к ПДн.

Совокупность таких условий и факторов формируется с учетом характеристик ИСПДн, свойств среды (пути) распространения информативных сигналов, содержащих защищаемую информацию, и возможностей источников угрозы.

К характеристикам ИСПДн, обусловливающим возникновение УБПДн, можно отнести категорию и объем обрабатываемых в ИСПДн персональных данных, структуру ИСПДн, наличие подключений ИСПДн к сетям связи общего пользования и (или) сетям международного информационного обмена, характеристики подсистемы безопасности ПДн, обрабатываемых в ИСПДн, режимы обработки персональных данных, режимы разграничения прав доступа пользователей ИСПДн, местонахождение и условия размещения технических средств ИСПДн.

Информационные системы ПДн представляют собой совокупность информационных и программно-аппаратных элементов, а также информационных технологий, применяемых при обработке ПДн.

Основными элементами ИСПДн являются:

- персональные данные, содержащиеся в базах данных, как совокупность информации и ее носителей, используемых в ИСПДн;
- информационные технологии, применяемые при обработке ПДн;
- технические средства, осуществляющие обработку ПДн (средства вычислительной

техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки ПДн, средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации) (далее - технические средства ИСПДн);

- программные средства (операционные системы, системы управления базами данных и т.п.);
- средства защиты информации;
- вспомогательные технические средства и системы (ВТСС) - технические средства и системы, их коммуникации, не предназначенные для обработки ПДн, но размещенные в помещениях (далее - служебные помещения), в которых расположены ИСПДн, их технические средства (различного рода телефонные средства и системы, средства вычислительной техники, средства и системы передачи данных в системе радиосвязи, средства и системы охранной и пожарной сигнализации, средства и системы оповещения и сигнализации, контрольно-измерительная аппаратура, средства и системы кондиционирования, средства и системы проводной радиотрансляционной сети и приема программ радиовещания и телевидения, средства электронной оргтехники, средства и системы электрочасофикации).

Свойства среды (пути) распространения информативных сигналов, содержащих защищаемую информацию, характеризуются видом физической среды, в которой распространяются ПДн, и определяются при оценке возможности реализации УБПДн.

Возможности источников УБПДн обусловлены совокупностью способов несанкционированного и (или) случайного доступа к ПДн, в результате которого возможно нарушение конфиденциальности (копирование, неправомерное распространение), целостности (уничтожение, изменение) и доступности (блокирование) ПДн.

Угроза безопасности ПДн реализуется в результате образования канала реализации УБПДн между источником угрозы и носителем (источником) ПДн, что создает условия для нарушения безопасности ПДн (несанкционированный или случайный доступ).

Основными элементами канала реализации УБПДн (рисунок 1) являются:

- источник УБПДн - субъект, материальный объект или физическое явление, создающие УБПДн;
- среда (путь) распространения ПДн или воздействий, в которой физическое поле, сигнал, данные или программы могут распространяться и воздействовать на защищаемые свойства (конфиденциальность, целостность, доступность) ПДн;
- носитель ПДн - физическое лицо или материальный объект, в том числе физическое поле, в котором ПДн находят свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

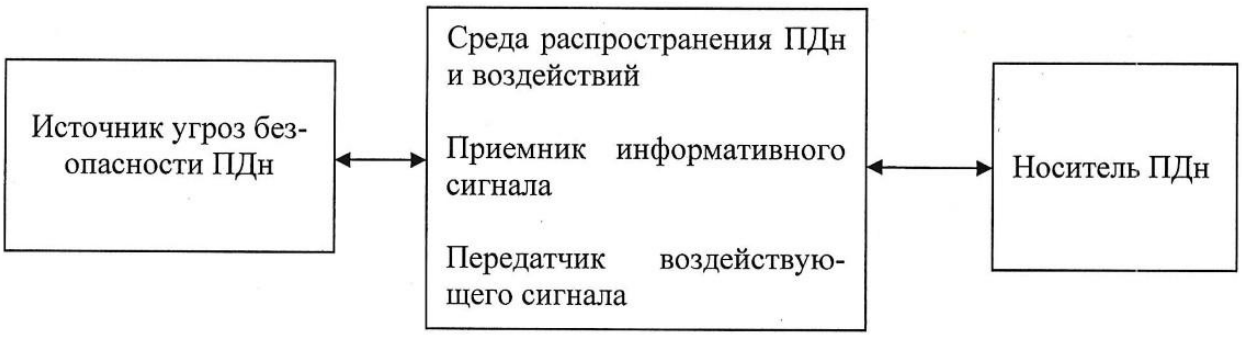


Рисунок 1. Обобщенная схема канала реализации угроз безопасности персональных данных

Носители ПДн могут содержать информацию, представленную в следующих видах:

- акустическая (речевая) информация (РИ), содержащаяся непосредственно в

произносимой речи пользователя ИСПДн при осуществлении им функции голосового ввода ПДн в ИСПДн, либо воспроизводимая акустическими средствами ИСПДн (если такие функции предусмотрены технологией обработки ПДн), а также содержащаяся в электромагнитных полях и электрических сигналах, которые возникают за счет преобразований акустической информации;

- видовая информация (ВИ), представленная в виде текста и изображений различных устройств отображения информации средств вычислительной техники, информационно-вычислительных комплексов, технических средств обработки графической, видео- и буквенно-цифровой информации, входящих в состав ИСПДн;
- информация, обрабатываемая (циркулирующая) в ИСПДн, в виде электрических, электромагнитных, оптических сигналов;
- информация, обрабатываемая в ИСПДн, представленная в виде бит, байт, файлов и других логических структур.

В целях формирования систематизированного перечня УБПДн при их обработке в ИСПДн угрозы классифицируются в соответствии со следующими признаками (рисунок 2):

- - по виду защищаемой от УБПДн информации, содержащей ПДн;
- - по видам возможных источников УБПДн;
- - по типу ИСПДн, на которые направлена реализация УБПДн;
- - по способу реализации УБПДн;
- - по виду нарушаемого свойства информации (виду несанкционированных действий, осуществляемых с ПДн);
- - по используемой уязвимости;
- - по объекту воздействия.

По видам возможных источников УБПДн выделяются следующие классы угроз:

- угрозы, связанные с преднамеренными или непреднамеренными действиями лиц, имеющих доступ к ИСПДн, включая пользователей ИСПДн, реализующих угрозы непосредственно в ИСПДн (внутренний нарушитель);
- угрозы, связанные с преднамеренными или непреднамеренными действиями лиц, не имеющих доступа к ИСПДн, реализующих угрозы из внешних сетей связи общего пользования и (или) сетей международного информационного обмена (внешний нарушитель).

Кроме того, угрозы могут возникать в результате внедрения аппаратных закладок и вредоносных программ.

По типу ИСПДн, на которые направлена реализация УБПДн, выделяются следующие классы угроз:

- угрозы безопасности ПДн, обрабатываемых в ИСПДн на базе автономного автоматизированного рабочего места (АРМ);
- угрозы безопасности ПДн, обрабатываемых в ИСПДн на базе АРМ, подключенного к сети общего пользования (к сети международного информационного обмена);
- угрозы безопасности ПДн, обрабатываемых в ИСПДн на базе локальных информационных систем без подключения к сети общего пользования (к сети международного информационного обмена);
- угрозы безопасности ПДн, обрабатываемых в ИСПДн на базе локальных информационных систем с подключением к сети общего пользования (к сети международного информационного обмена);
- угрозы безопасности ПДн, обрабатываемых в ИСПДн на базе распределенных информационных систем без подключения к сети общего пользования (к сети международного информационного обмена).

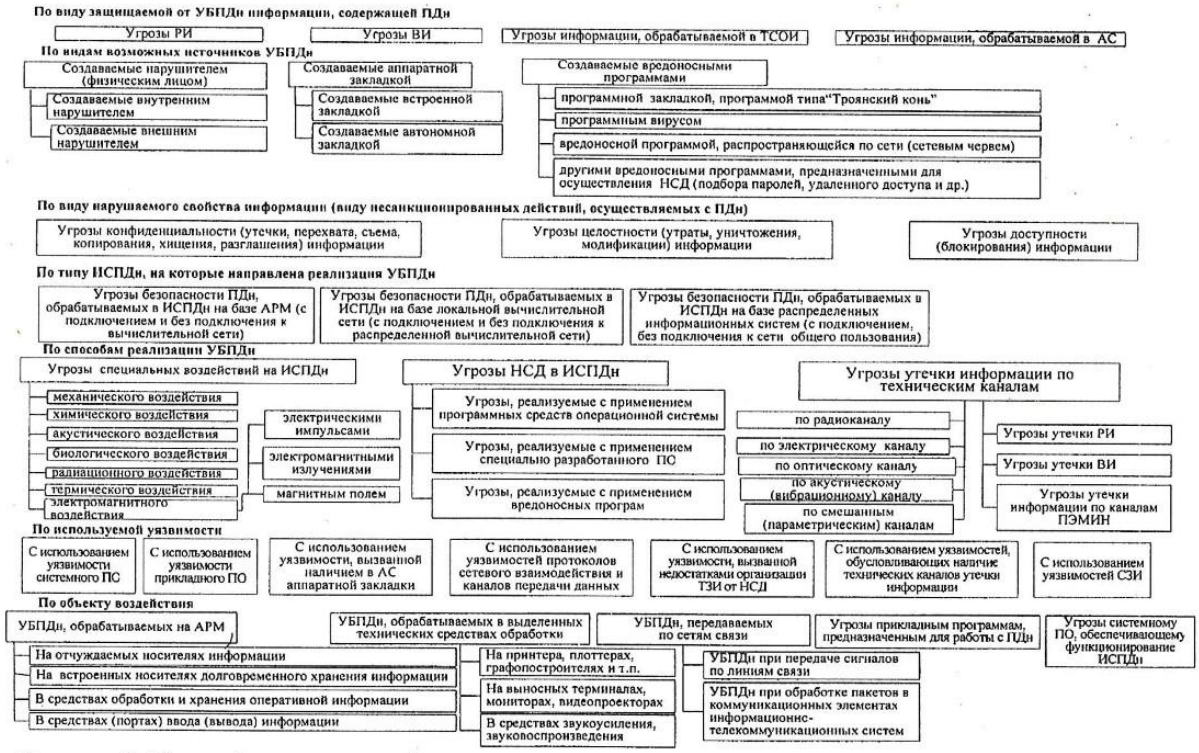


Рисунок 2. Классификация угроз безопасности персональных данных

Классификация угроз безопасности персональных данных, обрабатываемых в информационных системах персональных данных угрозы безопасности ПДн, обрабатываемых в ИСПДн на базе распределенных информационных систем с подключением к сети общего пользования (к сети международного информационного обмена).

По способам реализации УБПДн выделяются следующие классы угроз:

- угрозы, связанные с НСД к ПДн (в том числе угрозы внедрения вредоносных программ);
- угрозы утечки ПДн по техническим каналам утечки информации;
- угрозы специальных воздействий на ИСПДн.

По виду несанкционированных действий, осуществляемых с ПДн, выделяются следующие классы угроз:

- угрозы, приводящие к нарушению конфиденциальности ПДн (копированию или несанкционированному распространению), при реализации которых не осуществляется непосредственного воздействия на содержание информации;
- угрозы, приводящие к несанкционированному, в том числе случайному, воздействию на содержание информации, в результате которого осуществляется изменение ПДн или их уничтожение;
- угрозы, приводящие к несанкционированному, в том числе случайному, воздействию на программные или программно-аппаратные элементы ИСПДн, в результате которого осуществляется блокирование ПДн.

По используемой уязвимости выделяются следующие классы угроз:

- угрозы, реализуемые с использованием уязвимости системного ПО;
- угрозы, реализуемые с использованием уязвимости прикладного ПО;
- угрозы, возникающие в результате использования уязвимости, вызванной наличием в АС аппаратной закладки;
- угрозы, реализуемые с использованием уязвимостей протоколов сетевого взаимодействия и каналов передачи данных;
- угрозы, возникающие в результате использования уязвимости, вызванной недостатками организации ТЗИ от НСД;

- угрозы, реализуемые с использованием уязвимостей, обусловливающих наличие технических каналов утечки информации;
- угрозы, реализуемые с использованием уязвимостей СЗИ.

По объекту воздействия выделяются следующие классы угроз:

- угрозы безопасности ПДн, обрабатываемых на АРМ;
- угрозы безопасности ПДн, обрабатываемых в выделенных средствах обработки (принтерах, плоттерах, графопостроителях, вынесенных мониторах, видеопроекторах, средствах звуковоспроизведения и т.п.);
- угрозы безопасности ПДн, передаваемых по сетям связи;
- угрозы прикладным программам, с помощью которых обрабатываются ПДн;
- угрозы системному ПО, обеспечивающему функционирование ИСПДн.

Реализация одной из УБПДн перечисленных классов или их совокупности может привести к следующим типам последствий для субъектов ПДн:

- значительным негативным последствиям для субъектов ПДн;
- негативным последствиям для субъектов ПДн;
- незначительным негативным последствиям для субъектов ПДн.

Угрозы утечки ПДн по техническим каналам однозначно описываются характеристиками источника информации, среды (пути) распространения и приемника информативного сигнала, то есть определяются характеристиками технического канала утечки ПДн.

Угрозы, связанные с несанкционированным доступом (НСД) (далее - угрозы НСД в ИСПДн), представляются в виде совокупности обобщенных классов возможных источников угроз НСД, уязвимостей программного и аппаратного обеспечения ИСПДн, способов реализации угроз, объектов воздействия (носителей защищаемой информации, директориев, каталогов, файлов с ПДн или самих ПДн) и возможных деструктивных действий. Такое представление описывается следующей формализованной записью:

угроза НСД: = <источник угрозы>, <уязвимость программного или аппаратного обеспечения>, <способ реализации угрозы>, <объект воздействия>, <несанкционированный доступ>.

4. Угрозы утечки информации по техническим каналам

Основными элементами описания угроз утечки информации по техническим каналам (ТКУИ) являются: источник угрозы, среда (путь) распространения информативного сигнала и носитель защищаемой информации.

Источниками угроз утечки информации по техническим каналам являются физические лица, не имеющие доступа к ИСПДн, а также зарубежные спецслужбы или организации (в том числе конкурирующие или террористические), криминальные группировки, осуществляющие перехват (съем) информации с использованием технических средств ее регистрации, приема или фотографирования.

Среда распространения информативного сигнала – это физическая среда, по которой информативный сигнал может распространяться и приниматься (регистрироваться) приемником. Среда распространения может быть как однородной (например, только воздушной), так и неоднородной за счет перехода сигнала из одной среды в другую (например, в результате акустоэлектрических или виброакустических преобразований).

Носителем ПДн является пользователь ИСПДн, осуществляющий голосовой ввод ПДн в ИСПДн, акустическая система ИСПДн, воспроизводящая ПДн, а также технические средства ИСПДн и ВТСС, создающие физические поля, в которых информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

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

- угроз утечки акустической (речевой) информации;

- угроз утечки видовой информации;
- угроз утечки информации по каналам побочных электромагнитных излучений и наводок (ПЭМИН).

4.1. Угрозы утечки акустической (речевой) информации

Возникновение угроз утечки акустической (речевой) информации, содержащейся непосредственно в произносимой речи пользователя ИСПДн, при обработке ПДн в ИСПДн, обусловлено наличием функций голосового ввода ПДн в ИСПДн или функций воспроизведения ПДн акустическими средствами ИСПДн.

Перехват акустической (речевой) информации в данных случаях возможен с использованием аппаратуры, регистрирующей акустические (в воздухе) и виброакустические (в упругих средах) волны, а также электромагнитные (в том числе оптические) излучения и электрические сигналы, модулированные информативным акустическим сигналом, возникающие за счет преобразований в технических средствах обработки ПДн, ВТСС и строительных конструкциях и инженерно-технических коммуникациях под воздействием акустических волн.

Кроме этого, перехват акустической (речевой) информации возможен с использованием специальных электронных устройств съема речевой информации, внедренных в технические средства обработки ПДн, ВТСС и помещения или подключенных к каналам связи.

Угрозы безопасности ПДн, связанные с перехватом акустической информации с использованием специальных электронных устройств съема речевой информации («закладочных устройств»), определяются в соответствии с нормативным документами Федеральной службы безопасности Российской Федерации в установленном ею порядке.

Перехват акустической (речевой) информации может вестись:

- стационарной аппаратурой, размещаемой в близлежащих строениях (зданиях) с неконтролируемым пребыванием посторонних лиц;
- портативной возимой аппаратурой, размещаемой в транспортных средствах, осуществляющих движение вблизи служебных помещений или при их парковке рядом с этими помещениями;
- портативной носимой аппаратурой - физическими лицами при их неконтролируемом пребывании в служебных помещениях или в непосредственной близости от них;
- автономной автоматической аппаратурой, скрытно устанавливаемой физическими лицами непосредственно в служебных помещениях или в непосредственной близости от них.

4.2. 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.

Угрозы безопасности ПДн, связанные с их перехватом при использовании специальных электронных устройств съема видовой информации (видеозакладок), определяются в соответствии с нормативным документами Федеральной службы безопасности Российской Федерации в установленном ею порядке.

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

Перехват ПДн может вестись:

- стационарной аппаратурой, размещаемой в близлежащих строениях (зданиях) с неконтролируемым пребыванием посторонних лиц;
- портативной возимой аппаратурой, размещаемой в транспортных средствах, осуществляющих движение вблизи служебных помещений или при их парковке рядом с этими помещениями;
- портативной носимой аппаратурой - физическими лицами при их неконтролируемом пребывании в служебных помещениях или в непосредственной близости от них.

Перехват (просмотр) ПДн может осуществляться посторонними лицами путем их непосредственного наблюдения в служебных помещениях либо с расстояния прямой видимости из-за пределов ИСПДн с использованием оптических (оптикоэлектронных) средств.

4.3. Угрозы утечки информации по каналам побочных электромагнитных излучений и наводок

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 ПД 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, обрабатывающих ПДн (в средствах вычислительной техники, информационно-вычислительных комплексах и сетях, средствах и системах передачи, приема и обработки ПДн, в том числе в 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.

Кроме этого, перехват ПЭМИН возможен с использованием электронных устройств перехвата информации, подключенных к каналам связи или техническим средствам обработки ПДн.

Регистрация ПЭМИН может вестись с использованием аппаратуры следующих видов:

- стационарной аппаратурой, размещаемой в близлежащих строениях (зданиях) с неконтролируемым пребыванием посторонних лиц;
- портативной возимой аппаратуры, размещаемой в транспортных средствах, осуществляющих движение вблизи служебных помещений или при их парковке рядом с этими помещениями;
- портативной носимой аппаратурой - физическими лицами в непосредственной близости от ИСПДн;
- автономной автоматической аппаратурой, скрытно устанавливаемой физическими лицами в непосредственной близости от ИСПДн.

Каналы утечки информации, обусловленные наводками, образуются за счет соединительных линий технических средств ИСПДн и ВТСС и посторонних проводников (в том числе цепей электропитания и заземления).

Наводки электромагнитных излучений технических средств ИСПДн возникают при излучении элементами технических средств ИСПДн информативных сигналов при наличии

емкостной, индуктивной или гальванической связей соединительных линий технических средств ИСПДн, линий ВТСС и посторонних проводников. В результате на случайных антеннах (цепях ВТСС или посторонних проводниках) наводится информативный сигнал.

Прохождение информативных сигналов в цепи электропитания возможно при наличии емкостной, индуктивной или гальванической связи источника информативных сигналов в составе технических средств ИСПДн и цепей питания.

Прохождение информативных сигналов в цепи заземления обусловлено наличием емкостной, индуктивной или гальванической связи источника информативных сигналов в составе аппаратуры ТСПИ и цепей заземления.

Для съема информации с проводных линий могут использоваться:

- средства съема сигналов, содержащих защищаемую информацию, с цепей технических средств ИСПДн и ВТСС, линий связи и передачи данных, выходящих за пределы служебных помещений (эквиваленты сети, токовые трансформаторы, пробники);
- средства съема наведенных информативных сигналов с цепей электропитания;
- средства съема наведенных информативных сигналов с шин заземления;
- средства съема наведенных информативных сигналов с проводящих инженерных коммуникаций.

Для волоконно-оптической системы передачи данных угрозой утечки информации является утечка оптического излучения, содержащего защищаемую информацию, с боковой поверхности оптического волокна.

Появление новых каналов связи - сотовой связи, пейджинговых сообщений, спутниковых и беспроводных сетей передачи данных - привело к развитию специализированных систем и средств контроля и перехвата информации, ориентированных на используемые в них информационные технологии, в том числе средств:

перехвата пейджинговых сообщений и сотовой связи;

перехвата информации в каналах передачи данных вычислительных сетей.

5. Угрозы несанкционированного доступа к информации в информационной системе персональных данных

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:

- угрозы доступа (проникновения) в операционную среду компьютера с использованием штатного программного обеспечения (средств операционной системы или прикладных программ общего применения);
- угрозы создания нештатных режимов работы программных (программно-аппаратных) средств за счет преднамеренных изменений служебных данных, игнорирования предусмотренных в штатных условиях ограничений на состав и характеристики обрабатываемой информации, искажения (модификации) самих данных и т.п.;
- угрозы внедрения вредоносных программ (программно-математического воздействия).

Состав элементов описания угроз НСД к информации в ИСПДн приведен на рисунке 3.

Кроме этого, возможны комбинированные угрозы, представляющие собой сочетание указанных угроз. Например, за счет внедрения вредоносных программ могут создаваться условия для НСД в операционную среду компьютера, в том числе путем формирования нетрадиционных информационных каналов доступа.

Угрозы доступа (проникновения) в операционную среду ИСПДн с использованием штатного программного обеспечения разделяются на угрозы непосредственного и

удаленного доступа. Угрозы непосредственного доступа осуществляются с использованием программных и программно-аппаратных средств ввода/вывода компьютера. Угрозы удаленного доступа реализуются с использованием протоколов сетевого взаимодействия.

Эти угрозы реализуются относительно ИСПДн как на базе автоматизированного рабочего места, не включенного в сети связи общего пользования, так и применительно ко всем ИСПДн, имеющим подключение к сетям связи общего пользования и сетям международного информационного обмена.

Описание угроз доступа (проникновения) в операционную среду компьютера формально может быть представлено следующим образом:

угроза НСД в ИСПДн: = <источник угрозы>, <уязвимость ИСПДн>, <способ реализации угрозы>, <объект воздействия (программа, протокол, данные и др.)>, <деструктивное действие>.

Угрозы создания нештатных режимов работы программных (программно-аппаратных) средств – это угрозы «Отказа в обслуживании». Как правило, данные угрозы рассматриваются применительно к ИСПДн на базе локальных и распределенных информационных систем вне зависимости от подключения информационного обмена. Их реализация обусловлена тем, что при разработке системного или прикладного программного обеспечения не учитывается возможность преднамеренных действий по целенаправленному изменению:

- содержания служебной информации в пакетах сообщений, передаваемых по сети;
- условий обработки данных (например, игнорирование ограничений на длину пакета сообщения);
- форматов представления данных (с несоответствием измененных форматов, установленных для обработки по протоколам сетевого взаимодействия);
- программного обеспечения обработки данных.

В результате реализации угроз «Отказа в обслуживании» происходит переполнение буферов и блокирование процедур обработки, «зацикливание» процедур обработки и «зависание» компьютера, отбрасывание пакетов сообщений и др. Описание таких угроз формально может быть представлено следующим образом:

угроза «Отказа в обслуживании»: = <источник угрозы>, <уязвимость ИСПДн>, <способ реализации угрозы>, <объект воздействия (носитель ПДн)>, <непосредственный результат реализации угрозы (переполнение буфера, блокирование процедуры обработки, «зацикливание» обработки и т.п.)>.

Угрозы внедрения вредоносных программ (программно-математического воздействия) нецелесообразно описывать с той же детальностью, что и вышеуказанные угрозы. Это обусловлено тем, что, во-первых, количество вредоносных программ сегодня уже значительно превышает сто тысяч. Во-вторых, при организации защиты информации на практике, как правило, достаточно лишь знать класс вредоносной программы, способы и последствия от ее внедрения (инфицирования). В связи с этим угрозы программно-математического воздействия (ПМВ) формально могут быть представлены следующим образом:

угроза ПМВ в ИСПДн: = <класс вредоносной программы (с указанием среды обитания)>, <источник угрозы (носитель вредоносной программы)>, <способ инфицирования>, <объект воздействия (загрузочный сектор, файл и т.п.)>, <описание возможных деструктивных действий>, <дополнительная информация об угрозе (резидентность, скорость распространения, полиморфичность и др.)>.

Ниже дается общая характеристика источников угроз безопасности информации, уязвимостей, которые могут быть использованы при реализации угроз НСД, и характеристика результатов несанкционированного или случайного доступа. Характеристика способов реализации угроз дается при описании угроз доступа (проникновения) в операционную среду компьютера, угроз отказа в обслуживании и угроз ПМВ.

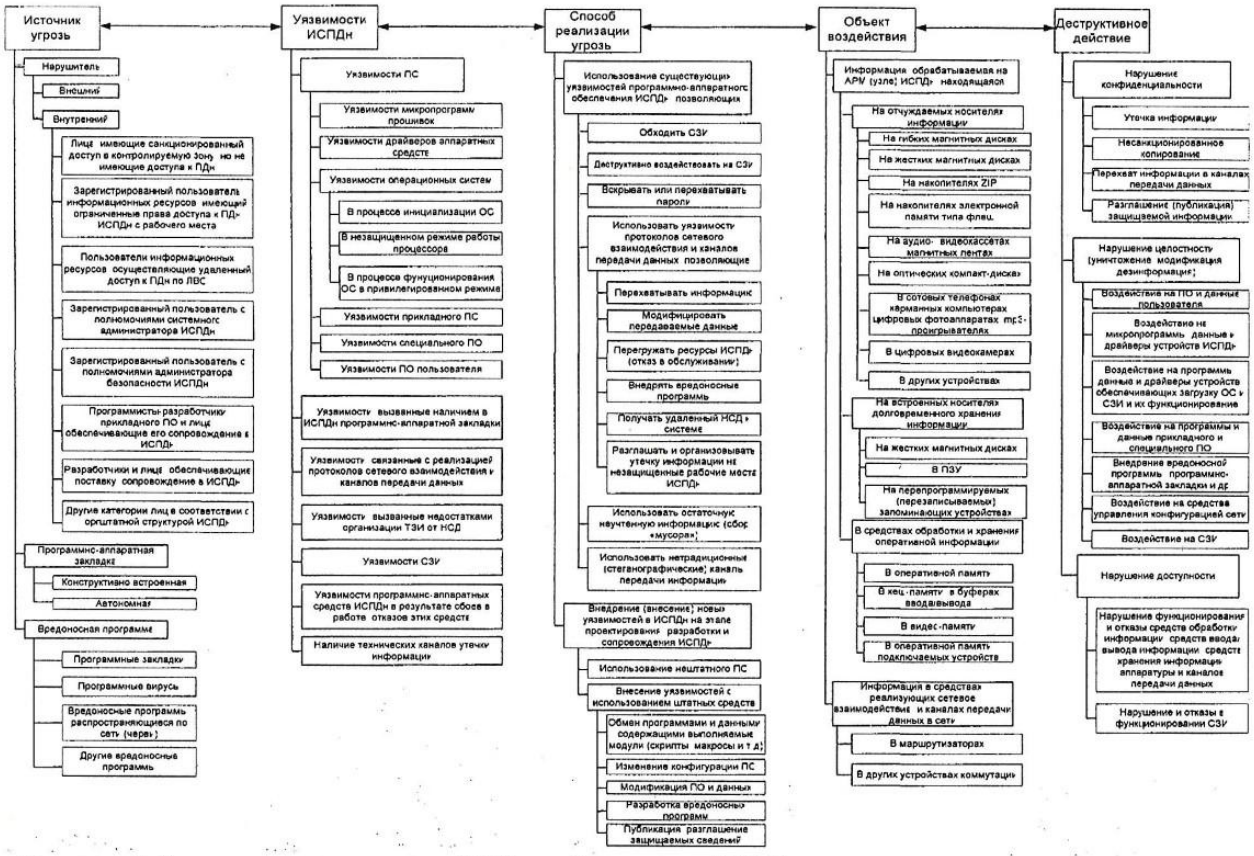


Рисунок 3. Элементы описания угроз НДС к информации в ИСПДн

5.1. Общая характеристика источников угроз несанкционированного доступа в информационной системе персональных данных

Источниками угроз НСД в ИСПДн могут быть:

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

Угрозы безопасности ПДн, связанные с внедрением аппаратных закладок, определяются в соответствии с нормативным документами Федеральной службы безопасности Российской Федерации в установленном ею порядке.

По наличию права постоянного или разового доступа в контролируемую зону (КЗ) ИСПДн нарушители подразделяются на два типа:

- нарушители, не имеющие доступа к ИСПДн, реализующие угрозы из внешних сетей связи общего пользования и (или) сетей международного информационного обмена, - внешние нарушители;
- нарушители, имеющие доступ к ИСПДн, включая пользователей ИСПДн, реализующие угрозы непосредственно в ИСПДн, - внутренние нарушители.

Внешними нарушителями могут быть:

- разведывательные службы государств;
- криминальные структуры;
- конкуренты (конкурирующие организации);
- недобросовестные партнеры;
- внешние субъекты (физические лица).

Внешний нарушитель имеет следующие возможности:

- осуществлять несанкционированный доступ к каналам связи, выходящим за пределы служебных помещений;
- осуществлять несанкционированный доступ через автоматизированные рабочие

места, подключенные к сетям связи общего пользования и (или) сетям международного информационного обмена;

- осуществлять несанкционированный доступ к информации с использованием специальных программных воздействий посредством программных вирусов, вредоносных программ, алгоритмических или программных закладок;
- осуществлять несанкционированный доступ через элементы информационной инфраструктуры ИСПДн, которые в процессе своего жизненного цикла (модернизации, сопровождения, ремонта, утилизации) оказываются за пределами контролируемой зоны;
- осуществлять несанкционированный доступ через информационные системы взаимодействующих ведомств, организаций и учреждений при их подключении к ИСПДн.

Возможности внутреннего нарушителя существенным образом зависят от действующих в пределах контролируемой зоны режимных и организационно-технических мер защиты, в том числе по допуску физических лиц к ПДн и контролю порядка проведения работ.

Внутренние потенциальные нарушители подразделяются на восемь категорий в зависимости от способа доступа и полномочий доступа к ПДн.

К первой категории относятся лица, имеющие санкционированный доступ к ИСПДн, но не имеющие доступа к ПДн. К этому типу нарушителей относятся должностные лица, обеспечивающие нормальное функционирование ИСПДн.

Лицо этой категории, может:

- иметь доступ к фрагментам информации, содержащей ПДн и распространяющейся по внутренним каналам связи ИСПДн;
- располагать фрагментами информации о топологии ИСПДн (коммуникационной части подсети) и об используемых коммуникационных протоколах и их сервисах;
- располагать именами и вести выявление паролей зарегистрированных пользователей;
- изменять конфигурацию технических средств ИСПДн, вносить в нее программно-аппаратные закладки и обеспечивать съем информации, используя непосредственное подключение к техническим средствам ИСПДн.

Ко второй категории относятся зарегистрированные пользователи ИСПДн, осуществляющие ограниченный доступ к ресурсам ИСПДн с рабочего места.

Лицо этой категории:

- обладает всеми возможностями лиц первой категории;
- знает, по меньшей мере, одно легальное имя доступа;
- обладает всеми необходимыми атрибутами (например, паролем), обеспечивающими доступ к некоторому подмножеству ПДн;
- располагает конфиденциальными данными, к которым имеет доступ.

Его доступ, аутентификация и права по доступу к некоторому подмножеству ПДн должны регламентироваться соответствующими правилами разграничения доступа.

К третьей категории относятся зарегистрированные пользователи ИСПДн, осуществляющие удаленный доступ к ПДн по локальным и (или) распределенным информационным системам.

Лицо этой категории:

- обладает всеми возможностями лиц первой и второй категорий;
- располагает информацией о топологии ИСПДн на базе локальной и (или) распределенной информационной системы, через которую осуществляется доступ, и о составе технических средств ИСПДн;
- имеет возможность прямого (физического) доступа к фрагментам технических средств ИСПДн.

К четвертой категории относятся зарегистрированные пользователи ИСПДн с полномочиями администратора безопасности сегмента (фрагмента) ИСПДн.

Лицо этой категории:

- обладает всеми возможностями лиц предыдущих категорий;
- обладает полной информацией о системном и прикладном программном обеспечении, используемом в сегменте (фрагменте) ИСПДн;
- обладает полной информацией о технических средствах и конфигурации сегмента (фрагмента) ИСПДн;
- имеет доступ к средствам защиты информации и протоколирования, а также к отдельным элементам, используемым в сегменте (фрагменте) ИСПДн;
- имеет доступ ко всем техническим средствам сегмента (фрагмента) ИСПДн;
- обладает правами конфигурирования и административной настройки некоторого подмножества технических средств сегмента (фрагмента) ИСПДн.

К пятой категории относятся зарегистрированные пользователи с полномочиями системного администратора ИСПДн.

Лицо этой категории:

- обладает всеми возможностями лиц предыдущих категорий;
- обладает полной информацией о системном и прикладном программном обеспечении ИСПДн;
- обладает полной информацией о технических средствах и конфигурации ИСПДн;
- имеет доступ ко всем техническим средствам обработки информации и данным ИСПДн;
- обладает правами конфигурирования и административной настройки технических средств ИСПДн.

Системный администратор выполняет конфигурирование и управление программным обеспечением (ПО) и оборудованием, включая оборудование, отвечающее за безопасность защищаемого объекта: средства криптографической защиты информации, мониторинга, регистрации, архивации, защиты от НСД.

К шестой категории относятся зарегистрированные пользователи с полномочиями администратора безопасности ИСПДн.

Лицо этой категории:

- обладает всеми возможностями лиц предыдущих категорий;
- обладает полной информацией об ИСПДн;
- имеет доступ к средствам защиты информации и протоколирования и к части ключевых элементов ИСПДн;
- не имеет прав доступа к конфигурированию технических средств сети за исключением контрольных (инспекционных).

Администратор безопасности отвечает за соблюдение правил разграничения доступа, за генерацию ключевых элементов, смену паролей. Администратор безопасности осуществляет аудит тех же средств защиты объекта, что и системный администратор.

К седьмой категории относятся программисты-разработчики (поставщики) прикладного программного обеспечения и лица, обеспечивающие его сопровождение на защищаемом объекте.

Лицо этой категории:

- обладает информацией об алгоритмах и программах обработки информации на ИСПДн;
- обладает возможностями внесения ошибок, недекларированных возможностей, программных закладок, вредоносных программ в программное обеспечение ИСПДн на стадии ее разработки, внедрения и сопровождения;
- может располагать любыми фрагментами информации о топологии ИСПДн и технических средствах обработки и защиты ПДн, обрабатываемых в ИСПДн.

К восьмой категории относятся разработчики и лица, обеспечивающие поставку, сопровождение и ремонт технических средств на ИСПДн.

Лицо этой категории:

- обладает возможностями внесения закладок в технические средства ИСПДн на стадии их разработки, внедрения и сопровождения;
- может располагать любыми фрагментами информации о топологии ИСПДн и технических средствах обработки и защиты информации в ИСПДн.

Указанные категории нарушителей должны учитываться при оценке возможностей реализации УБПДн.

Носителем вредоносной программы может быть аппаратный элемент компьютера или программный контейнер. Если вредоносная программа не ассоциируется с какой-либо прикладной программой, то в качестве ее носителя рассматриваются:

- отчуждаемый носитель, то есть дискета, оптический диск (CD-R, CD-RW), флэш-память, отчуждаемый винчестер и т.п.;
- встроенные носители информации (винчестеры, микросхемы оперативной памяти, процессор, микросхемы системной платы, микросхемы устройств, встраиваемых в системный блок, - видеоадаптера, сетевой платы, звуковой платы, модема, устройств ввода/вывода магнитных жестких и оптических дисков, блока питания и т.п., микросхемы прямого доступа к памяти, шин передачи данных, портов ввода/вывода);
- микросхемы внешних устройств (монитора, клавиатуры, принтера, модема, сканера и т.п.).

Если вредоносная программа ассоциируется с какой-либо прикладной программой, с файлами, имеющими определенные расширения или иные атрибуты, с сообщениями, передаваемыми по сети, то ее носителями являются:

- пакеты передаваемых по компьютерной сети сообщений;
- файлы (текстовые, графические, исполняемые и т.д.).

5.2. Общая характеристика уязвимостей информационной системы персональных данных

Уязвимость информационной системы персональных данных - недостаток или слабое место в системном или прикладном программном (программно-аппаратном) обеспечении автоматизированной информационной системы, которые могут быть использованы для реализации угрозы безопасности персональных данным.

Причинами возникновения уязвимостей являются:

- ошибки при проектировании и разработке программного (программно-аппаратного) обеспечения;
- преднамеренные действия по внесению уязвимостей в ходе проектирования и разработки программного (программно-аппаратного) обеспечения;
- неправильные настройки программного обеспечения, неправомерное изменение режимов работы устройств и программ;
- несанкционированное внедрение и использование неучтенных программ с последующим необоснованным расходованием ресурсов (загрузка процессора, захват оперативной памяти и памяти на внешних носителях);
- внедрение вредоносных программ, создающих уязвимости в программном и программно-аппаратном обеспечении;
- несанкционированные неумышленные действия пользователей, приводящие к возникновению уязвимостей;
- сбои в работе аппаратного и программного обеспечения (вызванные сбоями в электропитании, выходом из строя аппаратных элементов в результате старения и снижения надежности, внешними воздействиями электромагнитных полей технических устройств и др.).

Классификация основных уязвимостей ИСПДн приведена на рисунке 4.



Рисунок 4. Классификация уязвимостей программного обеспечения

Ниже представлена общая характеристика основных групп уязвимостей ИСПДн, включающих:

- уязвимости системного программного обеспечения (в том числе протоколов сетевого взаимодействия);
- уязвимости прикладного программного обеспечения (в том числе средств защиты информации).

5.2.1. Общая характеристика уязвимостей системного программного обеспечения

Уязвимости системного программного обеспечения необходимо рассматривать с привязкой к архитектуре построения вычислительных систем.

При этом возможны уязвимости:

- в микропрограммах, в прошивках ПЗУ, ППЗУ;
- в средствах операционной системы, предназначенных для управления локальными ресурсами ИСПДн (обеспечивающих выполнение функций управления процессами, памятью, устройствами ввода/вывода, интерфейсом с пользователем и т.п.), драйверах, утилитах;
- в средствах операционной системы, предназначенных для выполнения вспомогательных функций, - утилитах (архивирования, дефрагментации и др.), системных обрабатывающих программах (компиляторах, компоновщиках, отладчиках и т.п.), программах предоставления пользователю дополнительных услуг (специальных вариантах интерфейса, калькуляторах, играх и т.п.), библиотеках процедур различного назначения (библиотеках математических функций, функций ввода/вывода и т.д.);

- в средствах коммуникационного взаимодействия (сетевых средствах) операционной системы.

Уязвимости в микропрограммах и в средствах операционной системы, предназначенных для управления локальными ресурсами и вспомогательными функциями, могут представлять собой:

- функции, процедуры, изменение параметров которых определенным образом позволяет использовать их для несанкционированного доступа без обнаружения таких изменений операционной системой;
- фрагменты кода программ ("дыры", "люки"), введенные разработчиком, позволяющие обходить процедуры идентификации, аутентификации, проверки целостности и др.;
- отсутствие необходимых средств защиты (аутентификации, проверки целостности, проверки форматов сообщений, блокирования несанкционированно модифицированных функций и т.п.);
- ошибки в программах (в объявлении переменных, функций и процедур, в кодах программ), которые при определенных условиях (например, при выполнении логических переходов) приводят к сбоям, в том числе к сбоям функционирования средств и систем защиты информации.

Уязвимости протоколов сетевого взаимодействия связаны с особенностями их программной реализации и обусловлены ограничениями на размеры применяемого буфера, недостатками процедуры аутентификации, отсутствием проверок правильности служебной информации и др. Краткая характеристика этих уязвимостей применительно к протоколам приведена в таблице 2.

Таблица 2

Уязвимости отдельных протоколов стека протоколов TCP/IP, на базе которого функционируют глобальные сети общего пользования

Наименование протокола	Уровень стека протоколов	Наименование (характеристика) уязвимости	Содержание нарушения безопасности информации
FTP (File Transfer Protocol) - протокол передачи файлов по сети	Прикладной, представительный, сеансовый	1. Аутентификация на базе открытого текста (пароли пересылаются в незашифрованном виде) 2. Доступ по умолчанию 3. Наличие двух открытых портов	Возможность перехвата данных учетной записи (имен зарегистрированных пользователей, паролей). Получение удаленного доступа к хостам
telnet - протокол управления удаленным терминалом	Прикладной, представительный, сеансовый	Аутентификация на базе открытого текста (пароли пересылаются в незашифрованном виде)	Возможность перехвата данных учетной записи пользователя. Получение удаленного доступа к хостам
UDP - протокол передачи данных без установления соединения	Транспортный	Отсутствие механизма предотвращения перегрузок буфера	Возможность реализации UDP-шторма. В результате обмена пакетами происходит существенное снижение производительности сервера
ARP - протокол преобразования IP-адреса в	Сетевой	Аутентификация на базе открытого текста (информация пересылается в	Возможность перехвата трафика пользователя злоумышленником

физический адрес		незашифрованном виде)	
RIP - протокол маршрутной информации	Транспортный	Отсутствие аутентификации управляющих сообщений об изменении маршрута	Возможность перенаправления трафика через хост злоумышленника
TCP - протокол управления передачей	Транспортный	Отсутствие механизма проверки корректности заполнения служебных заголовков пакета	Существенное снижение скорости обмена и даже полный разрыв произвольных соединений по протоколу TCP
DNS - протокол установления соответствия мнемонических имен и сетевых адресов	Прикладной, представительный, сеансовый	Отсутствие средств проверки аутентификации полученных данных от источника	Фальсификация ответа DNS-сервера
IGMP - протокол передачи сообщений о маршрутизации	Сетевой	Отсутствие аутентификации сообщений об изменении параметров маршрута	Зависание систем Win 9x/NT/200
SMTP - протокол обеспечения сервиса доставки сообщений по электронной почте	Прикладной, представительный, сеансовый	Отсутствие поддержки аутентификации заголовков сообщений	Возможность подделывания сообщений электронной почты, а также адреса отправителя сообщения
SNMP - протокол управления маршрутизаторами в сетях	Прикладной, представительный, сеансовый	Отсутствие поддержки аутентификации заголовков сообщений	Возможность переполнения пропускной способности сети

Для систематизации описания множества уязвимостей используется единая база данных уязвимостей CVE (Common Vulnerabilities and Exposures), в разработке которой принимали участие специалисты многих известных компаний и организаций, таких как MITRE, ISS, Cisco, BindView, Axent, NFR, L-3, CyberSafe, CERT, Carnegie Mellon University, институт SANS и т.д. Эта база данных постоянно пополняется и используется при формировании баз данных многочисленных программных средств анализа защищенности и, прежде всего, сетевых сканеров.

5.2.2. Общая характеристика уязвимостей прикладного программного обеспечения

К прикладному программному обеспечению относятся прикладные программы общего пользования и специальные прикладные программы.

Прикладные программы общего пользования - текстовые и графические редакторы, медиапрограммы (аудио- и видеопроигрыватели, программные средства приема телевизионных программ и т.п.), системы управления базами данных, программные платформы общего пользования для разработки программных продуктов (типа Delphi, Visual Basic), средства защиты информации общего пользования и т.п.

Специальные прикладные программы – это программы, которые разрабатываются в интересах решения конкретных прикладных задач в данной ИСПДн (в том числе

программные средства защиты информации, разработанные для конкретной ИСПДн).

Уязвимости прикладного программного обеспечения могут представлять собой:

- функции и процедуры, относящиеся к разным прикладным программам и несовместимые между собой (не функционирующие в одной операционной среде) из-за конфликтов, связанных с распределением ресурсов системы;
- функции, процедуры, изменение определенным образом параметров которых позволяет использовать их для проникновения в операционную среду ИСПДн и вызова штатных функций операционной системы, выполнения несанкционированного доступа без обнаружения таких изменений операционной системой;
- фрагменты кода программ («дыры», «люки»), введенные разработчиком, позволяющие обходить процедуры идентификации, аутентификации, проверки целостности и др., предусмотренные в операционной системе;
- отсутствие необходимых средств защиты (аутентификации, проверки целостности, проверки форматов сообщений, блокирования несанкционированно модифицированных функций и т.п.);
- ошибки в программах (в объявлении переменных, функций и процедур, в кодах программ), которые при определенных условиях (например, при выполнении логических переходов) приводят к сбоям, в том числе к сбоям функционирования средств и систем защиты информации, к возможности несанкционированного доступа к информации.

Данные об уязвимостях разрабатываемого и распространяемого на коммерческой основе прикладного программного обеспечения собираются, обобщаются и анализируются в базе данных CVE*.

5.3. Общая характеристика угроз непосредственного доступа в операционную среду информационной системы персональных данных

Угрозы доступа (проникновения) в операционную среду компьютера и несанкционированного доступа к ПДн связаны с доступом:

- к информации и командам, хранящимся в базовой системе ввода/вывода (BIOS) ИСПДн, с возможностью перехвата управления загрузкой операционной системы и получением прав доверенного пользователя;
- в операционную среду, то есть в среду функционирования локальной операционной системы отдельного технического средства ИСПДн с возможностью выполнения несанкционированного доступа путем вызова штатных программ операционной системы или запуска специально разработанных программ, реализующих такие действия;
- в среду функционирования прикладных программ (например, к локальной системе управления базами данных);
- непосредственно к информации пользователя (к файлам, текстовой, аудио- и графической информации, полям и записям в электронных базах данных) и обусловлены возможностью нарушения ее конфиденциальности, целостности и доступности.

Эти угрозы могут быть реализованы в случае получения физического доступа к ИСПДн или, по крайней мере, к средствам ввода информации в ИСПДн. Их можно объединить по условиям реализации на три группы.

Первая группа включает в себя 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.

Вторая группа - 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 или какой-либо прикладной программы 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, и 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.

Наконец, третья группа включает в себя угрозы, реализация которых определяется тем, какая из прикладных программ запускается пользователем, или фактом запуска любой из прикладных программ. Большая часть таких угроз – это угрозы внедрения вредоносных программ.

5.4. Общая характеристика угроз безопасности персональных данных, реализуемых с использованием протоколов межсетевого взаимодействия

Если ИСПДн реализована на базе локальной или распределенной информационной системы, то в ней могут быть реализованы угрозы безопасности информации путем использования протоколов межсетевого взаимодействия. При этом может обеспечиваться НСД к ПДн или реализовываться угроза отказа в обслуживания. Особенно опасны угрозы, когда ИСПДн представляет собой распределенную информационную систему, подключенную к сетям общего пользования и (или) сетям международного информационного обмена. Классификационная схема угроз, реализуемых по сети, приведена на рисунке 5. В ее основу положено семь следующих первичных признаков классификации.

1. Характер угрозы. По этому признаку угрозы могут быть пассивные и активные. Пассивная угроза – это угроза, при реализации которой не оказывается непосредственное влияние на работу ИСПДн, но могут быть нарушены установленные правила разграничения доступа к ПДн или сетевым ресурсам. Примером таких угроз является угроза «Анализ сетевого трафика», направленная на прослушивание каналов связи и перехват передаваемой информации.

Активная угроза – это угроза, связанная с воздействием на ресурсы ИСПДн, при реализации которой оказывается непосредственное влияние на работу системы (изменение конфигурации, нарушение работоспособности и т.д.), и с нарушением установленных правил разграничения доступа к ПДн или сетевым ресурсам. Примером таких угроз является угроза «Отказ в обслуживании», реализуемая как «шторм TCP-запросов».

2. Цель реализации угрозы. По этому признаку угрозы могут быть направлены на нарушение конфиденциальности, целостности и доступности информации (в том числе на нарушение работоспособности ИСПДн или ее элементов).

3. Условие начала осуществления процесса реализации угрозы. По этому признаку может реализовываться угроза:

- по запросу от объекта, относительно которого реализуется угроза. В этом случае нарушитель ожидает передачи запроса определенного типа, который и будет условием начала осуществления несанкционированного доступа;



Рисунок 5. Классификационная схема угроз с использованием протоколов межсетевого взаимодействия

- по наступлению ожидаемого события на объекте, относительно которого реализуется угроза. В этом случае нарушитель осуществляет постоянное наблюдение за состоянием операционной системы ИСПДн и при возникновении определенного события в этой системе начинает несанкционированный доступ;
- безусловное воздействие. В этом случае начало осуществления несанкционированного доступа безусловно по отношению к цели доступа, то есть угроза реализуется немедленно и безотносительно к состоянию системы.

4. Наличие обратной связи с ИСПДн. По этому признаку процесс реализации угрозы может быть с обратной связью и без обратной связи. Угроза, осуществляемая при наличии обратной связи с ИСПДн, характеризуется тем, что на некоторые запросы, переданные на ИСПДн, нарушителю требуется получить ответ. Следовательно, между нарушителем и ИСПДн существует обратная связь, которая позволяет нарушителю адекватно реагировать на все изменения, происходящие в ИСПДн. В отличие от угроз, реализуемых при наличии обратной связи с ИСПДн, при реализации угроз без обратной связи не требуется реагировать на какие-либо изменения, происходящие в ИСПДн.

5. Расположение нарушителя относительно ИСПДн. В соответствии с этим признаком угроза реализуется как внутрисегментно, так и межсегментно. Сегмент сети - физическое объединение хостов (технических средств ИСПДн или коммуникационных элементов, имеющих сетевой адрес). Например, сегмент ИСПДн образует совокупность хостов, подключенных к серверу по схеме «общая шина». В случае, когда имеет место внутрисегментная угроза, нарушитель имеет физический доступ к аппаратным элементам ИСПДн. Если имеет место межсегментная угроза, то нарушитель располагается вне ИСПДн, реализуя угрозу из другой сети или из другого сегмента ИСПДн.

6. Уровень эталонной модели взаимодействия открытых систем** (ISO/OSI), на котором реализуется угроза. По этому признаку угроза может реализовываться на физическом, канальном, сетевом, транспортном, сеансовом, представительном и прикладном уровне модели ISO/OSI.

7. Соотношение количества нарушителей и элементов ИСПДн, относительно которых реализуется угроза. По этому признаку угроза может быть отнесена к классу угроз, реализуемых одним нарушителем относительно одного технического средства ИСПДн

(угроза «один к одному»), сразу относительно нескольких технических средств ИСПДн (угроза «один ко многим») или несколькими нарушителями с разных компьютеров относительно одного или нескольких технических средств ИСПДн (распределенные или комбинированные угрозы).

С учетом проведенной классификации можно выделить семь наиболее часто реализуемых в настоящее время угроз.

1. Анализ сетевого трафика (рисунок 6).

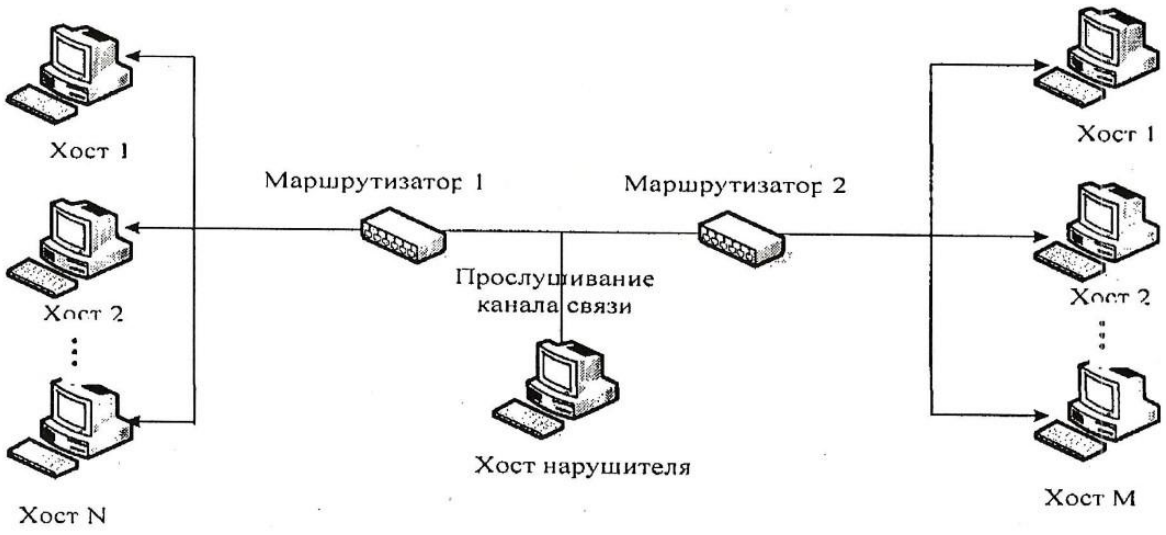


Рисунок 6. Схема реализации угрозы «Анализ сетевого трафика»

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. В ходе реализации угрозы нарушитель изучает логику работы сети - то есть стремится получить однозначное соответствие событий, происходящих в системе, и команд, пересылаемых при этом хостами, в момент появления данных событий. В дальнейшем это позволяет злоумышленнику на основе задания соответствующих команд получить, например, привилегированные права на действия в системе или расширить свои полномочия в ней, перехватить поток передаваемых данных, которыми обмениваются компоненты сетевой операционной системы, для извлечения конфиденциальной или идентификационной информации (например, статических паролей пользователей для доступа к удаленным хостам по протоколам FTP и TELNET, не предусматривающим шифрование), ее подмены, модификации и т.п.

2. Сканирование сети.

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

3. Угроза выявления пароля.

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.

4. Подмена доверенного объекта сети и передача по каналам связи сообщений от его имени с присвоением его прав доступа (рисунок 7). Такая угроза эффективно реализуется в системах, где применяются нестойкие алгоритмы идентификации и аутентификации хостов, пользователей и т.д. Под доверенным объектом понимается объект сети (компьютер, межсетевой экран, маршрутизатор и т.п.), легально подключенный к серверу.

Могут быть выделены две разновидности процесса реализации указанной угрозы: с установлением и без установления виртуального соединения.

Процесс реализации с установлением виртуального соединения состоит в присвоении прав доверенного субъекта взаимодействия, что позволяет нарушителю вести сеанс работы с объектом сети от имени доверенного субъекта. Реализация угрозы данного типа требует преодоления системы идентификации и аутентификации сообщений (например, атака rsh-службы UNIX-хоста).

Процесс реализации угрозы без установления виртуального соединения может иметь место в сетях, осуществляющих идентификацию передаваемых сообщений только по сетевому адресу отправителя. Сущность заключается в передаче служебных сообщений от имени сетевых управляющих устройств (например, от имени маршрутизаторов) об изменении маршрутно-адресных данных. При этом необходимо иметь в виду, что единственными идентификаторами абонентов и соединения (по протоколу TCP) являются два 32-битных параметра Initial Sequence Number - ISS (номер последовательности) и Acknowledgment Number - ACK (номер подтверждения). Следовательно, для формирования ложного TCP-пакета нарушителю необходимо знать текущие идентификаторы для данного соединения - ISSa и ISSb, где:

ISSa - некоторое численное значение, характеризующее порядковый номер отправляемого TCP-пакета, устанавливаемого TCP-соединения, инициированного хостом A;

ISSb - некоторое численное значение, характеризующее порядковый номер отправляемого TCP-пакета, устанавливаемого TCP-соединения, инициированного хостом B.

Значение ACK (номера подтверждения установления TCP-соединения) определяется как значение номера, полученного от респондента ISS (номер последовательности) плюс единица ACKb = ISSa + 1.

В результате реализации угрозы нарушитель получает права доступа, установленные его пользователем для доверенного абонента, к техническому средству ИСПДн - цели угроз.

5. Навязывание ложного маршрута сети.

Данная угроза реализуется одним из двух способов: путем внутрисегментного или межсегментного навязывания. 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 (рисунки 8 и 9).

6. Внедрение 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.

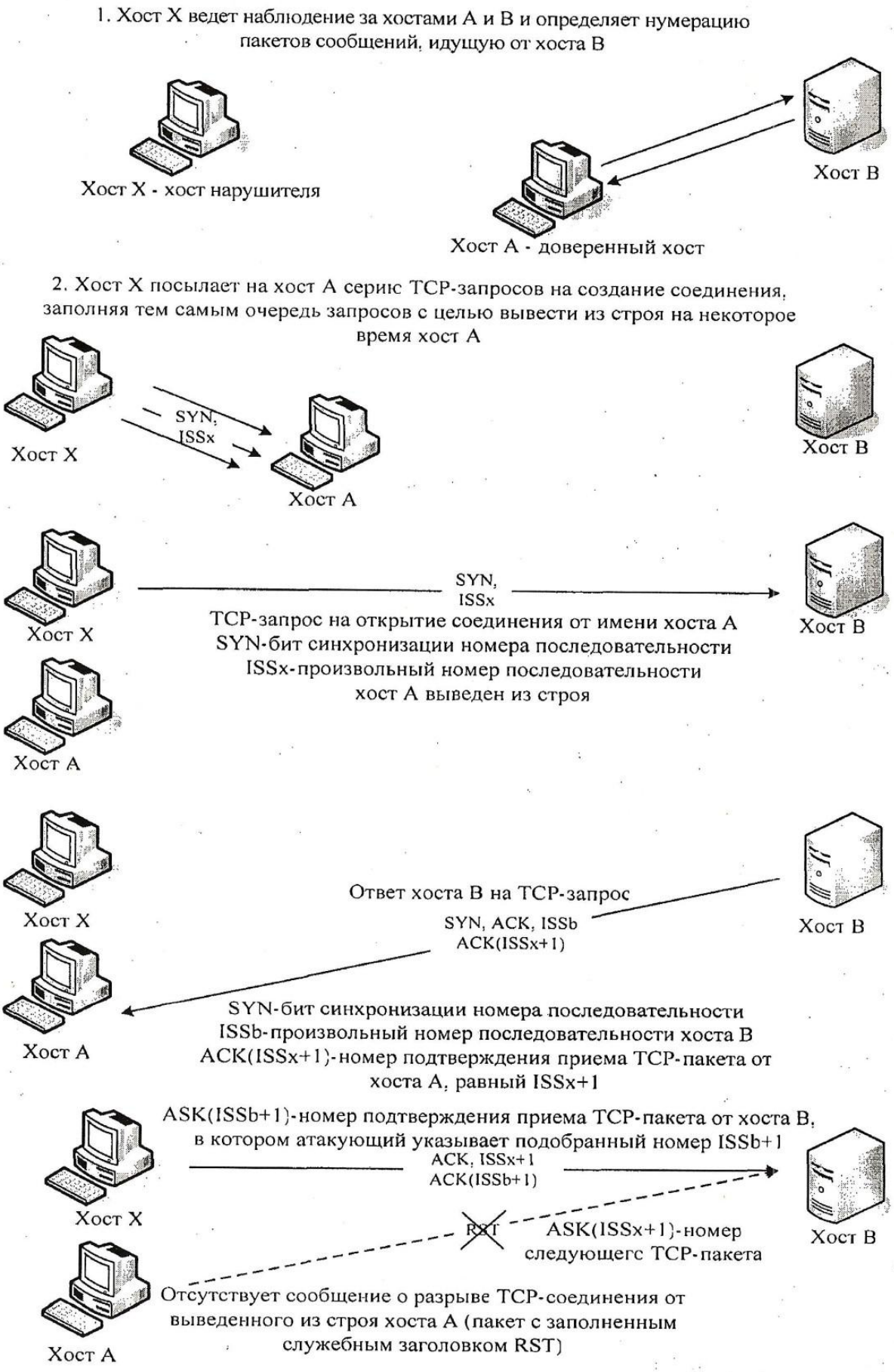


Рисунок 7. Схема реализации угрозы «Подмена доверенного объекта сети»

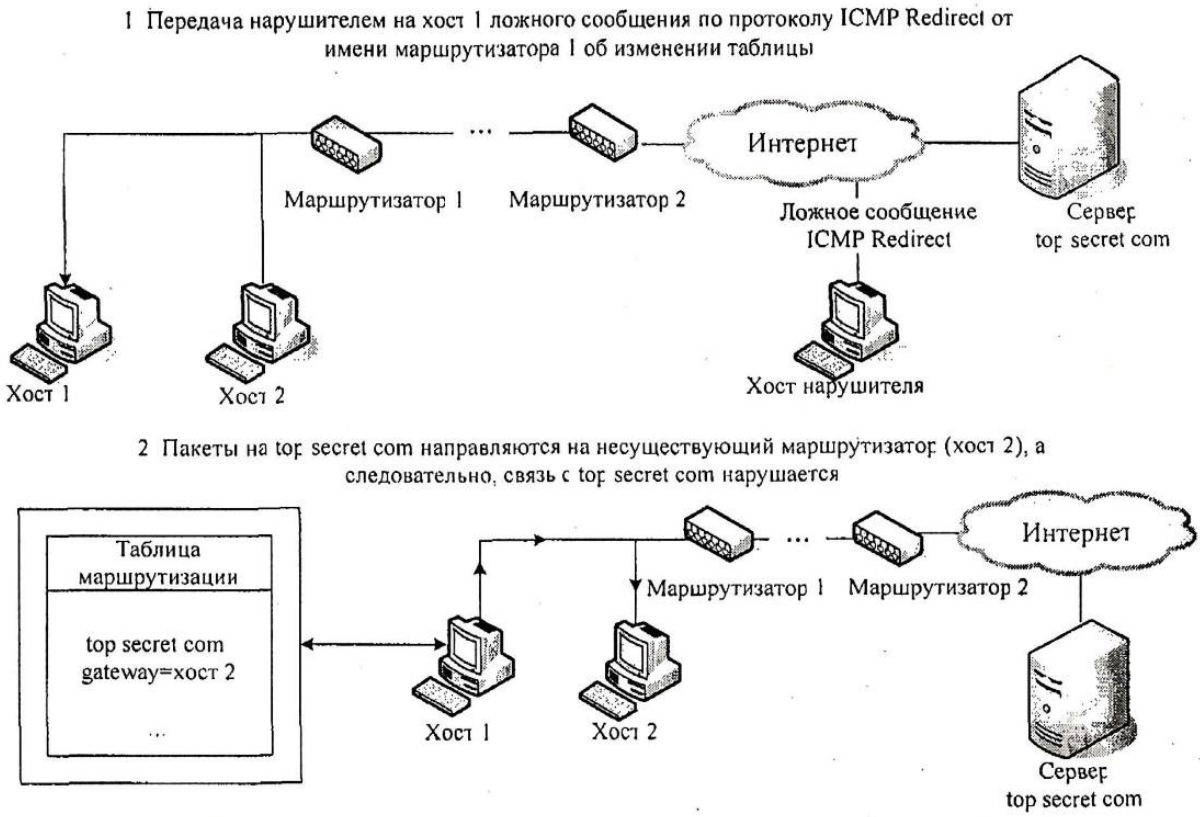


Рисунок 8. Схема реализации атаки «Навязывание ложного маршрута» (внутрисегментное) с использованием протокола ICMP с целью нарушения связи»

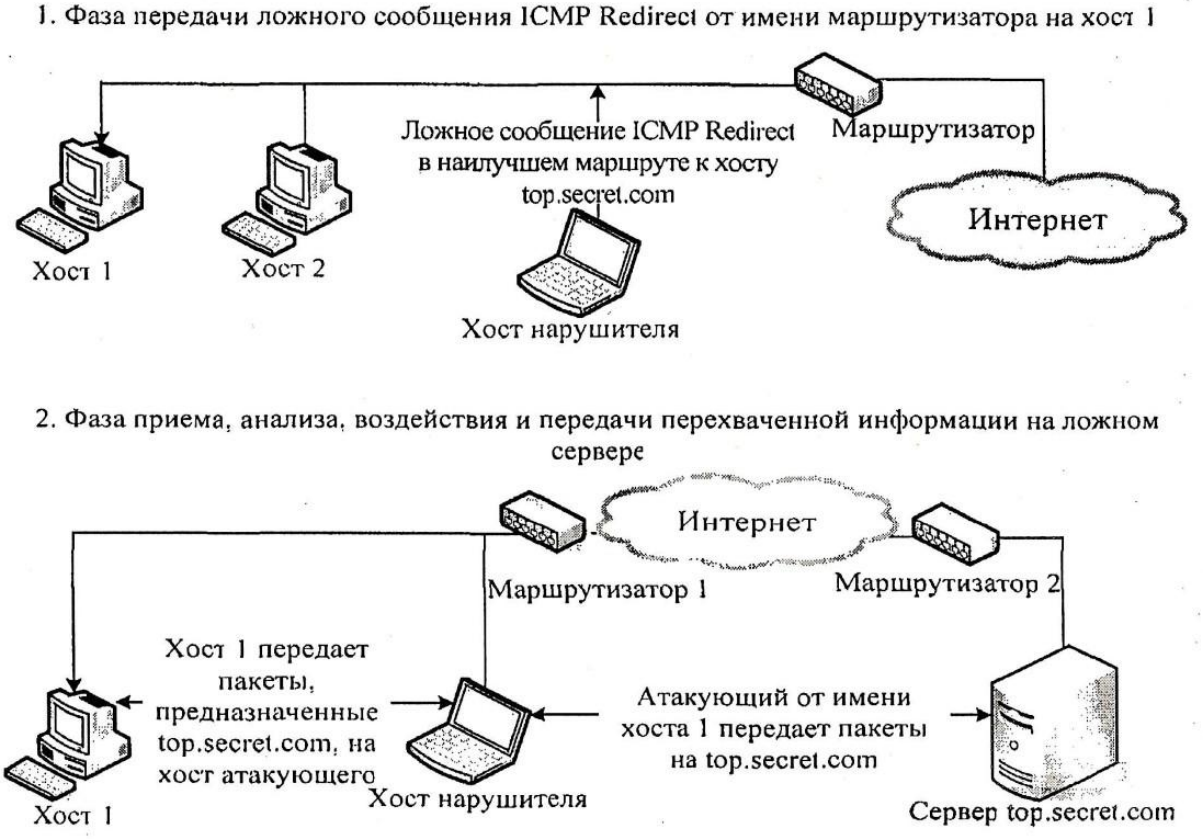


Рисунок 9. Схема реализации угрозы «Навязывание ложного маршрута» (межсегментное) с целью перехвата трафика»

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 (рисунки 10-13).

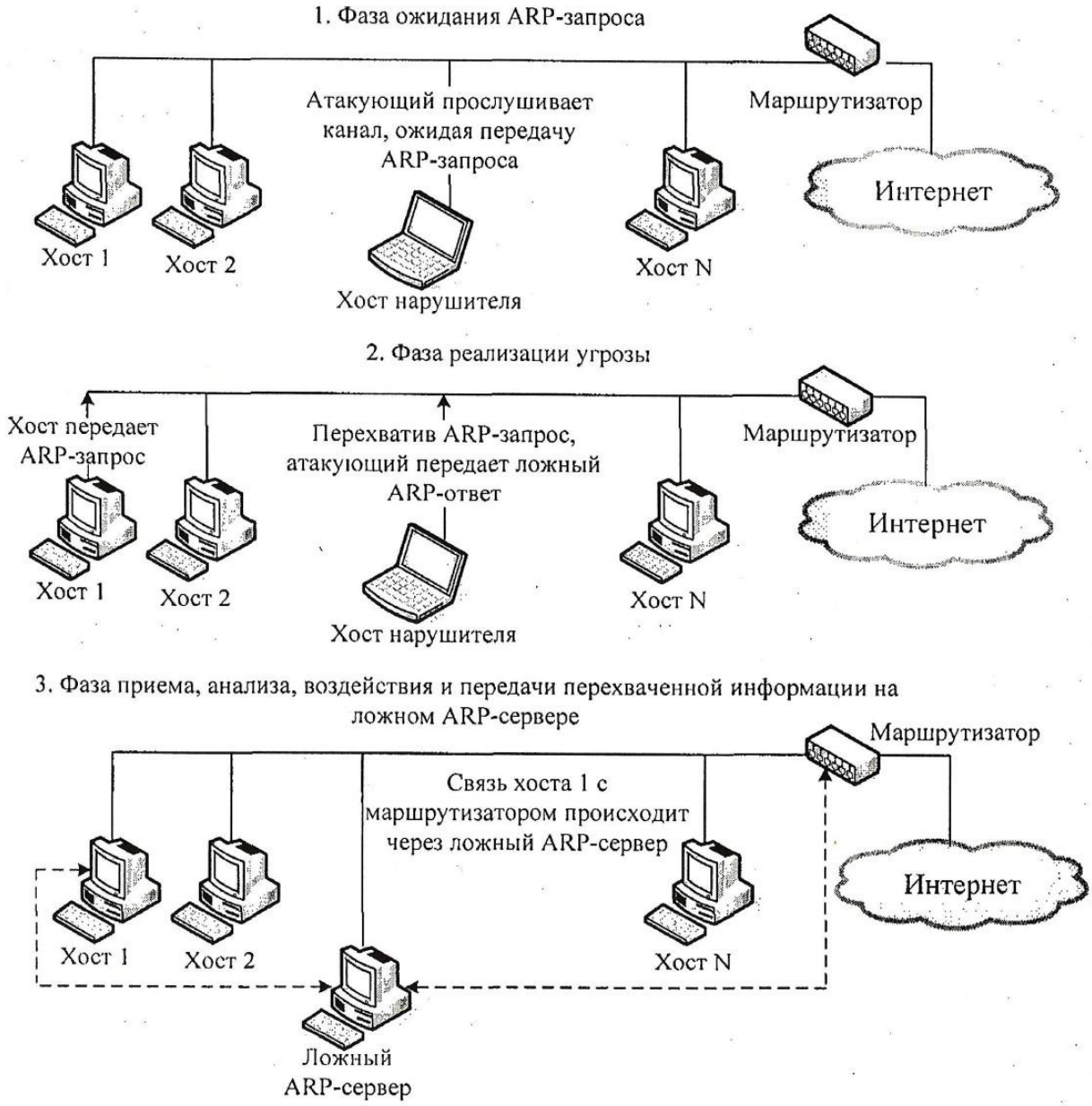
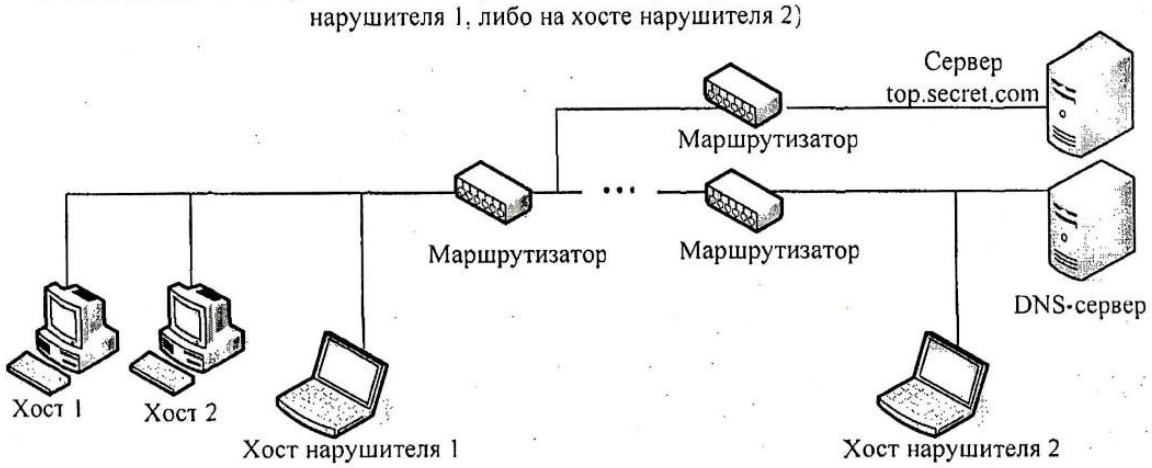
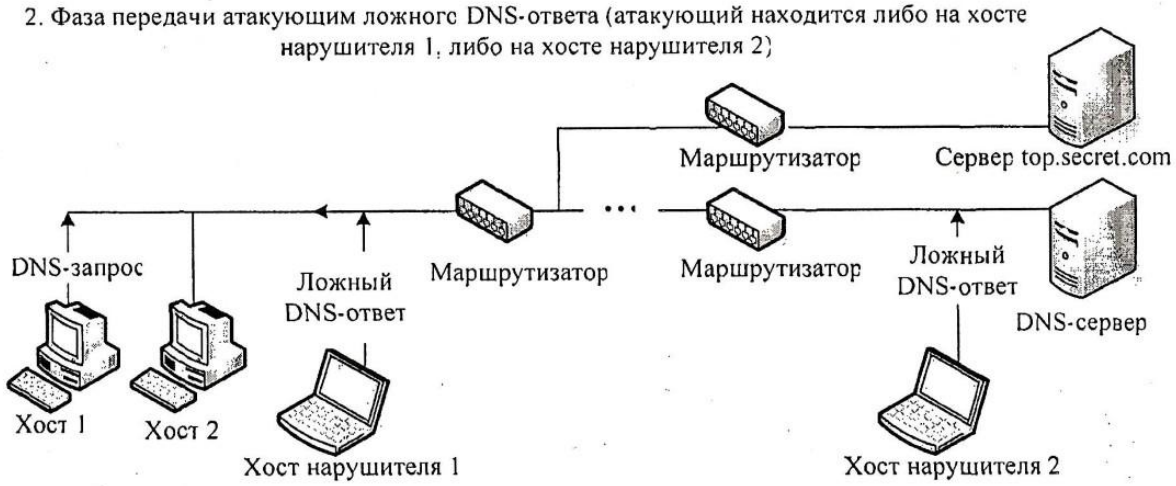


Рисунок 10. Схема реализации угрозы «Внедрение ложного ARP-сервера»

1. Фаза ожидания атакующим DNS-запроса от хоста 1 (атакующий находится либо на хосте нарушителя 1, либо на хосте нарушителя 2)



2. Фаза передачи атакующим ложного DNS-ответа (атакующий находится либо на хосте нарушителя 1, либо на хосте нарушителя 2)



3. Фаза приема, анализа, воздействия и передачи перехваченной информации на ложном сервере

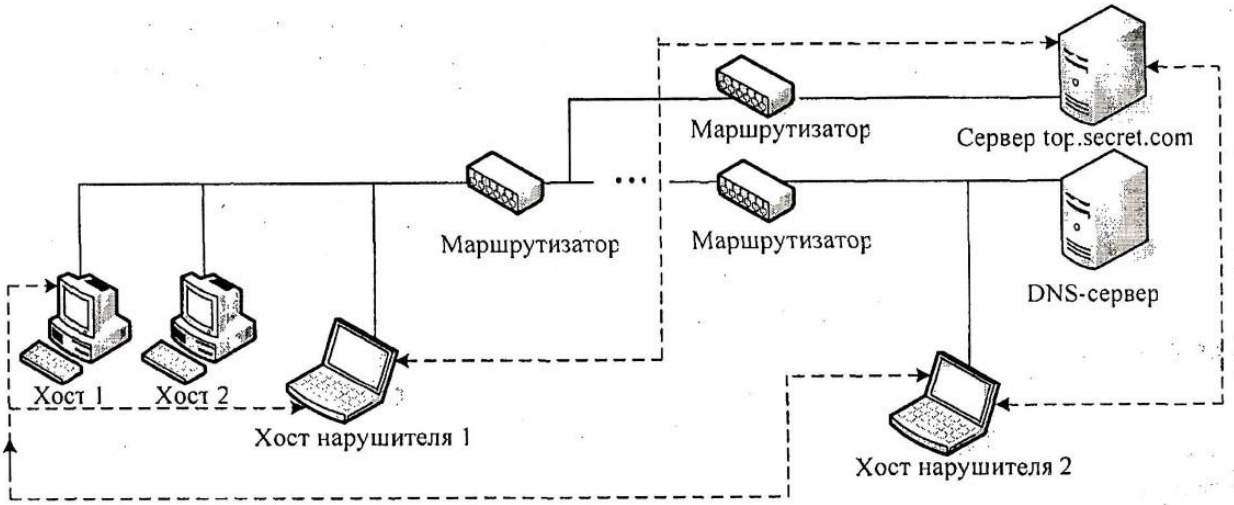
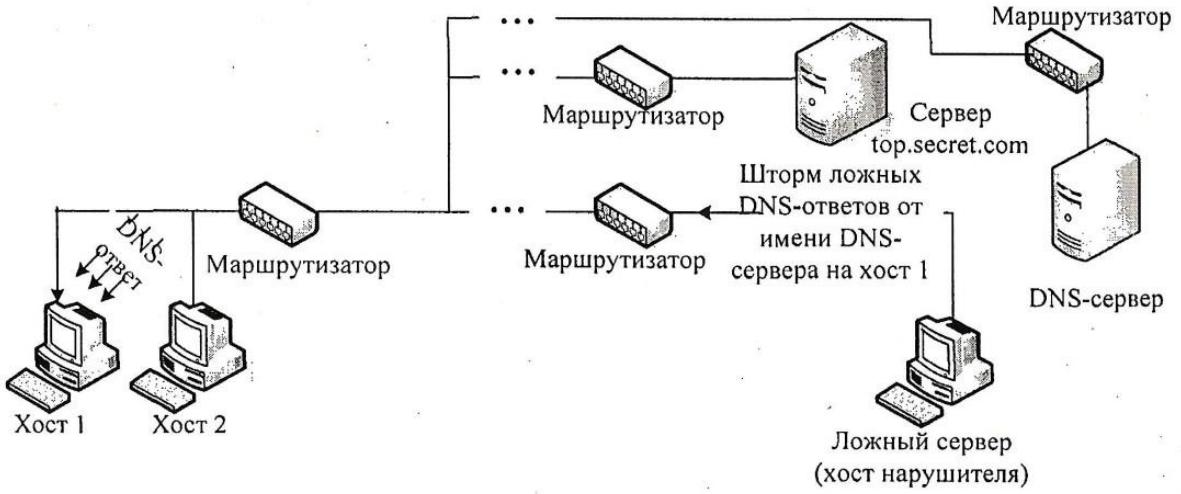
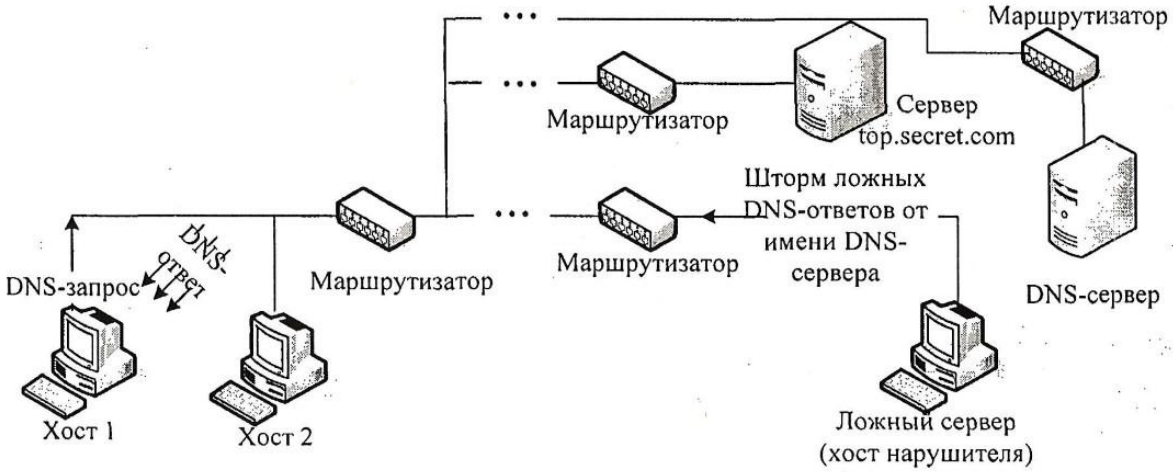


Рисунок 11. Схема реализации угрозы «Внедрение ложного DNS-сервера» путем перехвата DNS-запроса»

1. Нарушитель передает направленный шторм DNS-ответов на хост 1



2. Хост 1 посылает DNS-запрос и немедленно получает ложный DNS-ответ



3. Фаза приема, анализа, воздействия и передачи перехваченной информации на ложном сервере

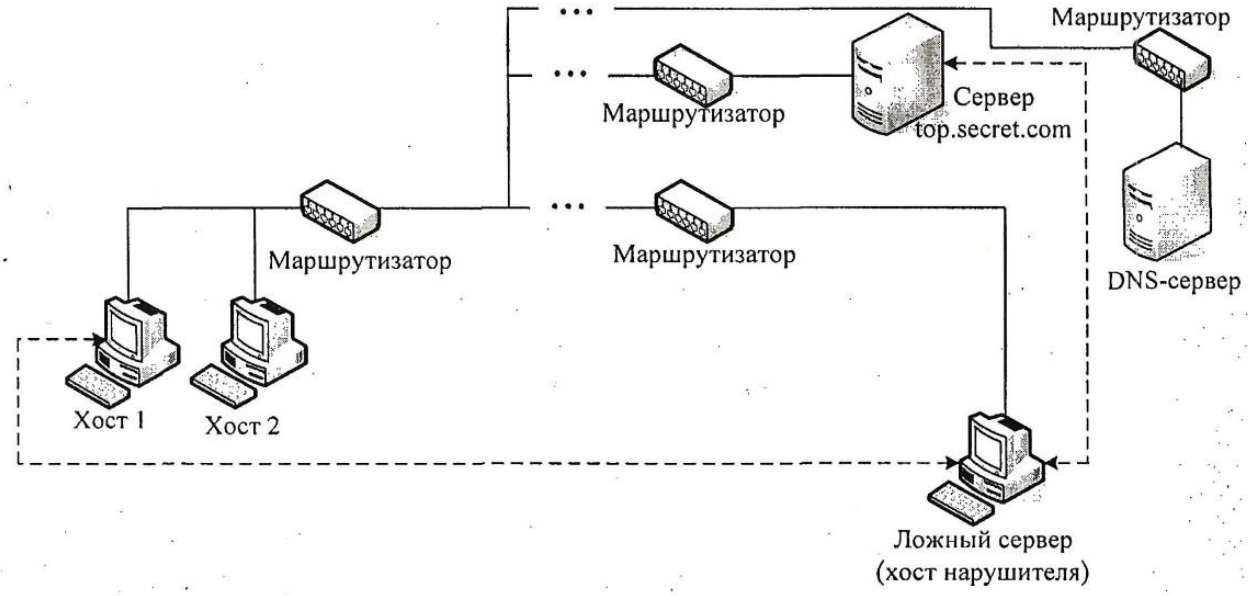
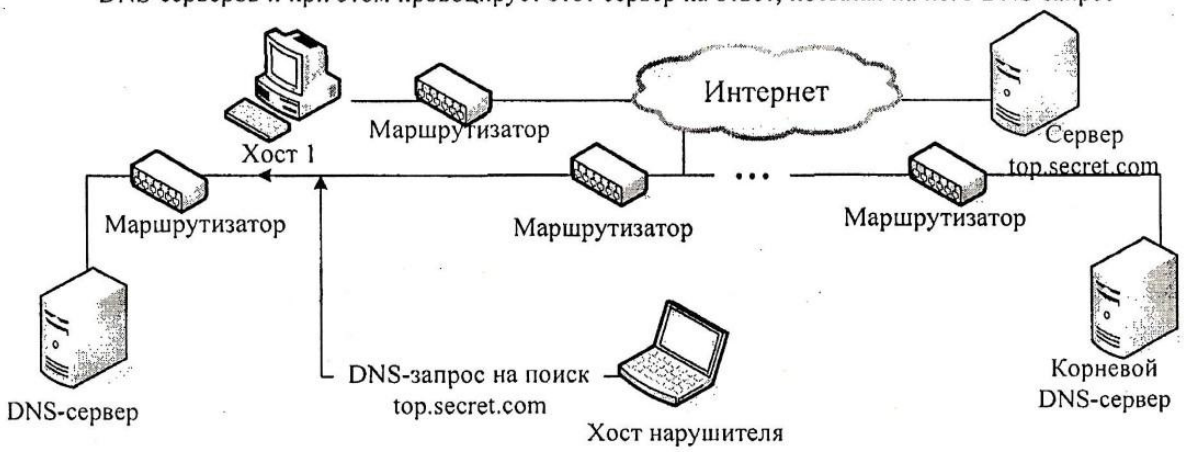
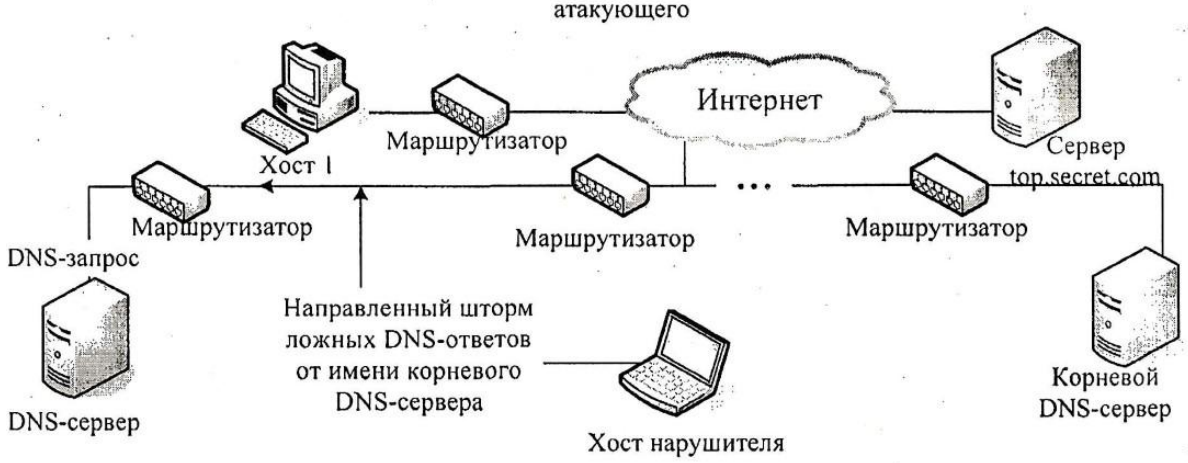


Рисунок 12. Схема реализации угрозы «внедрение ложного DNS-сервера» путем шторма DNS-ответов на компьютер сети»

1. Нарушитель создает направленный шторм ложных DNS-ответов от имени одного из корневых DNS-серверов и при этом провоцирует этот сервер на ответ, посылая на него DNS-запрос



2. DNS-сервер передает DNS-запрос на корневой DNS-сервер и немедленно получает ложный DNS-ответ от атакующего



3. Хост нарушителя изменяет кэш-таблицу DNS-сервера и обеспечивает прохождение трафика через ложный Сервер top.secret.com

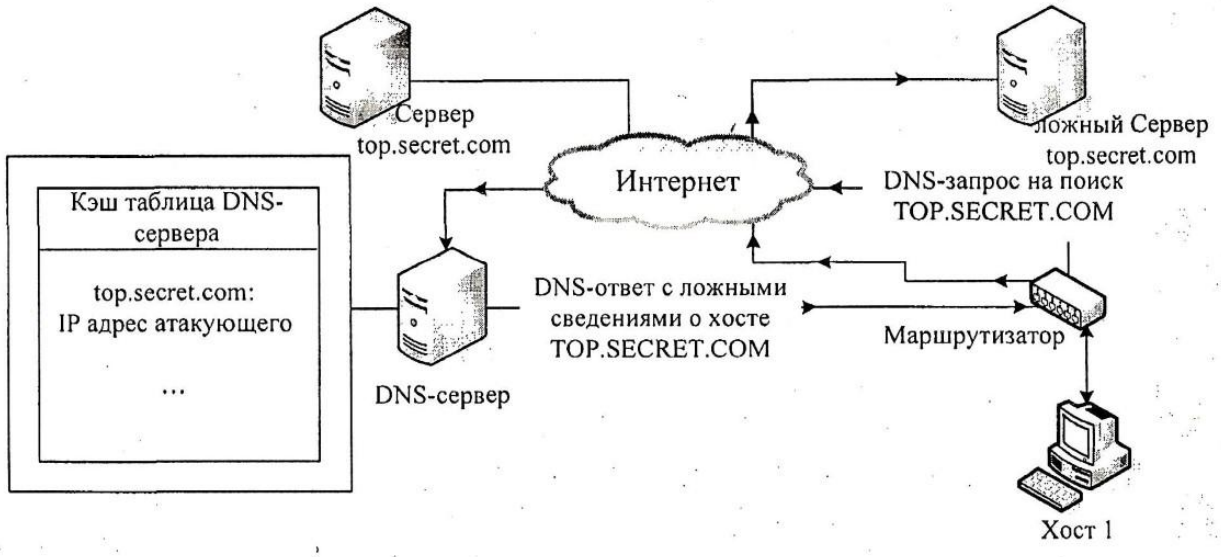


Рисунок 13. Схема реализации угрозы «Внедрение ложного DNS-сервера» путем шторма DNS-ответов на DNS-сервер»

7. 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.

Могут быть выделены несколько разновидностей таких угроз:

а) 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 ко времени обработки запросов. Примерами реализации угроз подобного рода могут служить: направленный шторм эхо-запросов по протоколу ICMP (Ping flooding), шторм запросов на установление TCP-соединений (SYN-flooding), шторм запросов к FTP-серверу;

б) явный отказ в обслуживании, вызванный 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);

в) 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;

г) явный отказ в обслуживании, вызванный передачей злоумышленником пакетов с нестандартными атрибутами (угрозы типа "Land", "TearDrop", "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 к 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 полную остановку компьютера из-за невозможности системы заниматься ничем другим, кроме обработки запросов.

8. Удаленный запуск приложений.

Угроза заключается в стремлении запустить на хосте ИСПДн различные предварительно внедренные вредоносные программы: программы-закладки, вирусы, "сетевые шпионы", основная цель которых - 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 данных угроз:

1) распространение файлов, содержащих несанкционированный исполняемый код;

2) удаленный запуск приложения путем переполнения буфера приложений-серверов;

3) удаленный запуск приложения путем использования возможностей удаленного управления системой, предоставляемых скрытыми программными и аппаратными закладками либо используемыми штатными средствами.

Типовые угрозы первого из указанных подклассов 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.

При угрозах второго подкласса используются недостатки программ, реализующих сетевые сервисы (в частности, отсутствие контроля переполнения 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».

При угрозах третьего подкласса нарушитель использует возможности удаленного управления системой, предоставляемые скрытыми компонентами (например, «троянскими» программами типа Back Orifice, Net Bus) либо штатными средствами управления и администрирования компьютерных сетей (Landesk Management Suite, Managewise, Back Orifice и т.п.). В результате их использования удается добиться удаленного контроля над станцией в сети.

Схематично основные этапы работы этих программ выглядят следующим образом:

- инсталляция в памяти;
- ожидание запроса с удаленного хоста, на котором запущена клиент-программа, и обмен с ней сообщениями о готовности;
- передача перехваченной информации клиенту или предоставление ему контроля над атакуемым компьютером.

Возможные последствия от реализации угроз различных классов приведены в таблице 3.

Таблица 3

Возможные последствия реализации угроз различных классов

№ п/п	Тип атаки	Возможные последствия
1	Анализ сетевого трафика	Исследование характеристик сетевого трафика, перехват передаваемых данных, в том числе идентификаторов и паролей пользователей
2	Сканирование сети	Определение протоколов, доступных портов сетевых служб, законов формирования идентификаторов соединений, активных сетевых сервисов, идентификаторов и паролей пользователей
3	"Парольная" атака	Выполнение любого деструктивного действия, связанного с получением несанкционированного доступа
4	Подмена доверенного объекта сети	Изменение трассы прохождения сообщений, несанкционированное изменение маршрутно-адресных данных. Несанкционированный доступ к сетевым ресурсам, навязывание ложной информации
5	Навязывание ложного маршрута	Несанкционированное изменение маршрутно-адресных данных, анализ и модификация передаваемых данных, навязывание ложных сообщений
6	Внедрение ложного объекта сети	Перехват и просмотр трафика. Несанкционированный доступ к сетевым ресурсам, навязывание ложной

			информации
7	Отказ в обслуживании	Частичное исчерпание ресурсов	Снижение пропускной способности каналов связи, производительности сетевых устройств. Снижение производительности серверных приложений
		Полное исчерпание ресурсов	Невозможность передачи сообщений из-за отсутствия доступа к среде передачи, отказ в установлении соединения. Отказ в предоставлении сервиса (электронной почты, файлового и т.д.)
		Нарушение логической связности между атрибутами, данными, объектами	Невозможность передачи, сообщений из-за отсутствия корректных маршрутно-адресных данных. Невозможность получения услуг ввиду несанкционированной модификации идентификаторов, паролей и т.п.
		Использование ошибок в программах	Нарушение работоспособности сетевых устройств
8	Удаленный запуск приложений	Путем рассылки файлов, содержащих деструктивный исполняемый код, вирусное заражение	Нарушение конфиденциальности, целостности, доступности информации
		Путем переполнения буфера серверного приложения	
		Путем использования возможностей удаленного управления системой, предоставляемых скрытыми программными и аппаратными закладками либо используемыми штатными средствами	Скрытое управление системой

Процесс реализации угрозы в общем случае состоит из четырех этапов:

- сбора информации;
- вторжения (проникновения в операционную среду);
- осуществления несанкционированного доступа;
- ликвидации следов несанкционированного доступа.

На этапе сбора информации нарушителя могут интересовать различные сведения об ИСПДн, в том числе:

а) о топологии сети, в которой функционирует система. При этом может исследоваться область вокруг сети (например, нарушителя могут интересовать адреса доверенных, но менее защищенных хостов). Для определения доступности хоста могут использоваться простейшие команды (например, команда ping для посылки ICMP-запросов

ECHO_REQUEST с ожиданием на них ICMP-ответов ECHO_REPLY). Существуют утилиты, осуществляющие параллельное определение доступности хостов (такие как fping), которые способны просканировать большую область адресного пространства на предмет доступности хостов за короткий промежуток времени. Топология сети часто определяется на основании «счетчика узлов» (дистанции между хостами). При этом могут применяться такие методы, как «модуляции TTL» и записи маршрута.

Метод «модуляции TTL» реализован программой traceroute (для Windows NT - tracert.exe) и заключается в модуляции поля TTL IP-пакетов. Для записи маршрута могут использоваться ICMP-пакеты, создаваемые командой ping.

Сбор информации может быть также основан на запросах:

к DNS-серверу о списке зарегистрированных (и, вероятно, активных) хостов;

- к маршрутизатору на основе протокола RIP об известных маршрутах (информация о топологии сети);
- к некорректно сконфигурированным устройствам, поддерживающим протокол SNMP (информация о топологии сети).

Если ИСПДн находится за межсетевым экраном (МЭ), возможен сбор информации о конфигурации МЭ и о топологии ИСПДн за МЭ, в том числе путем посылки пакетов на все порты всех предполагаемых хостов внутренней (защищаемой) сети;

б) о типе операционной системы (ОС) в ИСПДн. Самый известный способ определения типа ОС хоста основан на том, что различные типы ОС по-разному реализуют требования стандартов RFC к стеку TCP/IP. Это позволяет нарушителю удаленно идентифицировать тип ОС, установленной на хосте ИСПДн путем посылки специальным образом сформированных запросов и анализа полученных ответов.

Существуют специальные средства, реализующие данные методы, в частности, Nmap и QueSO. Можно отметить также такой метод определения типа ОС, как простейший запрос на установление соединения по протоколу удаленного доступа telnet (telnet-соединения), в результате которого по "внешнему виду" ответа можно определить тип ОС хоста. Наличие определенных сервисов также может служить дополнительным признаком для определения типа ОС хоста;

в) о функционирующих на хостах сервисах. Определение сервисов, исполняемых на хосте, основано на методе выявления "открытых портов", направленном на сбор информации о доступности хоста. Например, для определения доступности UDP-порта необходимо получить отклик в ответ на посылку UDP-пакета соответствующему порту:

- если в ответ пришло сообщение ICMP PORT UNREACHEBLE, то соответствующий сервис недоступен;
- если данное сообщение не поступило, то порт «открыт».

Возможны весьма разнообразные вариации использования этого метода в зависимости от используемого протокола в стеке протоколов TCP/IP.

Для автоматизации сбора информации об ИСПДн разработано множество программных средств. В качестве примера можно отметить следующие из них:

1) Strobe, Portscanner - оптимизированные средства определения доступных сервисов на основе опроса TCP-портов;

2) Nmap - средство сканирования доступных сервисов, предназначенное для ОС Linux, FreeBSD, Open BSD, Solaris, Windows NT. Является самым популярным в настоящее время средством сканирования сетевых сервисов;

3) Queso - высокоточное средство определения ОС хоста сети на основе посылки цепи корректных и некорректных TCP-пакетов, анализа отклика и сравнения его с множеством известных откликов различных ОС. Данное средство также является популярным на сегодняшний день средством сканирования;

4) Cheops - сканер топологии сети позволяет получить топологию сети, включая картину домена, области IP-адресов и т.д. При этом определяется ОС хоста, а также возможные сетевые устройства (принтеры, маршрутизаторы и т.д.);

5) Firewalk - сканер, использующий методы программы traceroute в интересах анализа отклика на IP-пакеты для определения конфигурации межсетевого экрана и построения топологии сети.

На этапе вторжения исследуется наличие типовых уязвимостей в системных сервисах или ошибок в администрировании системы. Успешным результатом использования уязвимостей обычно является получение процессом нарушителя привилегированного режима выполнения (доступа к привилегированному режиму выполнения командного процессора), внесение в систему учетной записи незаконного пользователя, получение файла паролей или нарушение работоспособности атакуемого хоста.

Этот этап развития угрозы, как правило, является многофазным. К фазам процесса реализации угрозы могут относиться, например:

- установление связи с хостом, относительно которого реализуется угроза;
- выявление уязвимости;
- внедрение вредоносной программы в интересах расширения прав и др.

Угрозы, реализуемые на этапе вторжения, подразделяются по уровням стека протоколов TCP/IP, поскольку формируются на сетевом, транспортном или прикладном уровне в зависимости от используемого механизма вторжения.

К типовым угрозам, реализуемым на сетевом и транспортном уровнях, относятся такие как:

а) угроза, направленная на подмену доверенного объекта;

б) угроза, направленная на создание в сети ложного маршрута;

в) угрозы, направленные на создание ложного объекта с использованием недостатков алгоритмов удаленного поиска;

г) угрозы типа «отказ в обслуживании», основанные на IP-дефрагментации, на формировании некорректных ICMP-запросов (например, атака "Ping of Death" и "Smurf"), на формировании некорректных TCP-запросов (атака "Land"), на создании "шторма" пакетов с запросами на соединение (атаки "SYN Flood") и др.

К типовым угрозам, реализуемым на прикладном уровне, относятся угрозы, направленные на несанкционированный запуск приложений, угрозы, реализация которых связана с внедрением программных закладок (типа «троянский конь»), с выявлением паролей доступа в сеть или к определенному хосту и т.д.

Если реализация угрозы не принесла нарушителю наивысших прав доступа в системе, возможны попытки расширения этих прав до максимально возможного уровня. Для этого могут использоваться уязвимости не только сетевых сервисов, но и уязвимости системного программного обеспечения хостов ИСПдн.

На этапе реализации несанкционированного доступа осуществляется собственно достижение цели реализации угрозы:

- нарушение конфиденциальности (копирование, неправомерное распространение);
- нарушение целостности (уничтожение, изменение);
- нарушение доступности (блокирование).

На этом же этапе, после указанных действий, как правило, формируется так называемый «черный вход» в виде одного из сервисов (демонов), обслуживающих некоторый порт и выполняющих команды нарушителя. «Черный вход» оставляется в системе в интересах обеспечения:

- возможности получить доступ к хосту, даже если администратор устранит использованную для успешной реализации угрозы уязвимость;
- возможности получить доступ к хосту как можно более скрытно;
- возможности получить доступ к хосту быстро (не повторяя заново процесс реализации угрозы).

«Черный вход» позволяет нарушителю внедрить в сеть или на определенный хост вредоносную программу, например, «анализатор паролей» (password sniffer) - программу, выделяющую пользовательские идентификаторы и пароли из сетевого трафика при работе

протоколов высокого уровня (ftp, telnet, rlogin и т.д.). Объектами внедрения вредоносных программ могут быть программы аутентификации и идентификации, сетевые сервисы, ядро операционной системы, файловая система, библиотеки и т.д.

Наконец, на этапе ликвидации следов реализации угрозы осуществляется попытка уничтожения следов действий нарушителя. При этом удаляются соответствующие записи из всех возможных журналов аудита, в том числе записи о факте сбора информации.

5.5. Общая характеристика угроз программно-математических воздействий

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 (копирование, уничтожение, блокирование 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.

Современные вредоносные программы основаны на использовании уязвимостей различного рода программного обеспечения (системного, общего, прикладного) и разнообразных сетевых технологий, обладают широким спектром деструктивных возможностей (от несанкционированного исследования параметров ИСПДн без вмешательства в функционирование ИСПДн, до уничтожения ПДн и программного обеспечения ИСПДн) и могут действовать во всех видах программного обеспечения (системного, прикладного, в драйверах аппаратного обеспечения и т.д.).

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 и криптографическую защиту.

Основными видами вредоносных программ являются:

- программные закладки;
- классические программные (компьютерные) вирусы;
- вредоносные программы, распространяющиеся по сети (сетевые черви);
- другие вредоносные программы, предназначенные для осуществления НСД.

К программным закладкам относятся программы, фрагменты кода, инструкции, формирующие недекларированные возможности программного обеспечения. Вредоносные программы могут переходить из одного вида в другой, например, программная закладка может сгенерировать программный вирус, который, в свою очередь, попав в условия сети,

может сформировать сетевого червя или другую вредоносную программу, предназначенную для осуществления НСД.

Классификация программных вирусов и сетевых червей представлена на рисунке 14. Краткая характеристика основных вредоносных программ сводится к следующему. Загрузочные вирусы записывают себя либо в загрузочный сектор диска (boot-сектор), либо в сектор, содержащий системный загрузчик винчестера (Master Boot Record), либо меняют указатель на активный boot-сектор. Они внедряются в память компьютера при загрузке с инфицированного диска. При этом системный загрузчик считывает содержимое первого сектора диска, с которого производится загрузка, помещает считанную информацию в память и передает на нее (т.е. на вирус) управление. После этого начинают выполняться инструкции вируса, который, как правило, уменьшает объем свободной памяти, копирует в освободившееся место свой код и считывает с диска свое продолжение (если оно есть), перехватывает необходимые вектора прерываний (обычно - INT 13H), считывает в память оригинальный boot-сектор и передает на него управление.

В дальнейшем загрузочный вирус ведет себя так же, как файловый: перехватывает обращения операционной системы к дискам и инфицирует их, в зависимости от некоторых условий совершает деструктивные действия, вызывает звуковые эффекты или видеоэффекты.

Основными деструктивными действиями, выполняемыми этими вирусами, являются:

- уничтожение информации в секторах дискет и винчестера;
- исключение возможности загрузки операционной системы (компьютер "зависает");
- искажение кода загрузчика;
- форматирование дискет или логических дисков винчестера;
- закрытие доступа к COM- и LPT-портам;
- замена символов при печати текстов;
- подергивания экрана;
- изменение метки диска или дискеты;
- создание псевдосбойных кластеров;
- создание звуковых и (или) визуальных эффектов (например, падение букв на экране);
- порча файлов данных;
- перезагрузка компьютера;
- вывод на экран разнообразных сообщений;
- отключение периферийных устройств (например, клавиатуры);
- изменение палитры экрана;
- заполнение экрана посторонними символами или изображениями;

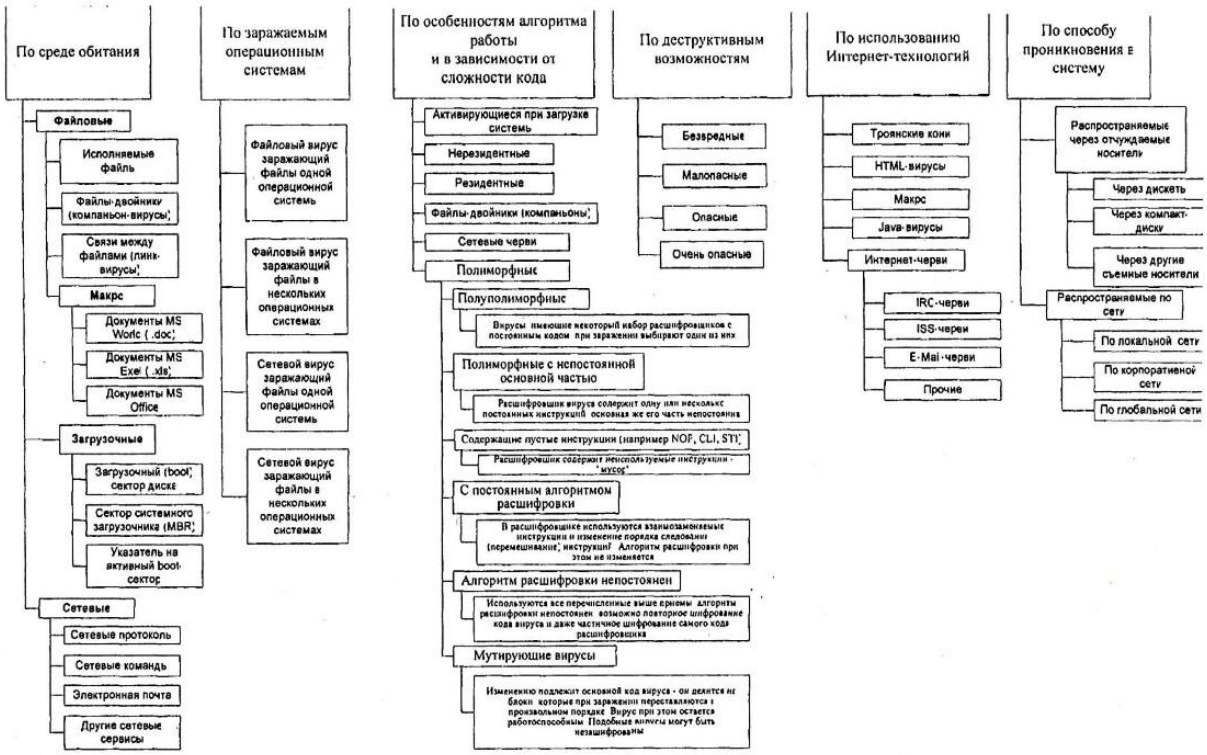


Рисунок 14. «Классификация программных вирусов и сетевых червей»

- погашение экрана и перевод в режим ожидания ввода с клавиатуры;
- шифрование секторов винчестера;
- выборочное уничтожение символов, выводимых на экран при наборе с клавиатуры;
- уменьшение объема оперативной памяти;
- вызов печати содержимого экрана;
- блокирование записи на диск;
- уничтожение таблицы разбиения (Disk Partition Table), после этого компьютер можно загрузить только с флоппи-диска;
- блокирование запуска исполняемых файлов;
- блокирование доступа к винчестеру.

Большинство загрузочных вирусов перезаписывают себя на флоппи-диски.

Файловые вирусы при своем размножении тем или иным способом используют файловую систему какой-либо операционной системы. По способу заражения файлов вирусы делятся на замещающие ("overwriting"), паразитические ("parasitic"), компаньон-вирусы ("companion"), "link"-вирусы, вирусы-черви и вирусы, заражающие объектные модули (OBJ), библиотеки компиляторов (LIB) и исходные тексты программ.

Метод заражения "overwriting" является наиболее простым: вирус записывает свой код вместо кода заражаемого файла, уничтожая его содержимое. Естественно, что при этом файл перестает работать и не восстанавливается. Такие вирусы очень быстро обнаруживают себя, так как операционная система и приложения довольно быстро перестают работать.

К паразитическим относятся все файловые вирусы, которые при распространении своих копий обязательно изменяют содержимое файлов, оставляя сами файлы при этом полностью или частично работоспособными. Основными типами таких вирусов являются вирусы, записывающиеся в начало, середину или конец файлов. Отдельно следует отметить довольно незначительную группу паразитических вирусов, не имеющих "точки входа" (EPO-вирусы - Entry Point Obscuring viruses). К ним относятся вирусы, не записывающие команду передачи управления в заголовок COM-файлов (JMP) и не изменяющие адрес точки старта в заголовке EXE-файлов. Такие вирусы записывают команду перехода на свой

код в какое-либо место в середину файла и получают управление не непосредственно при запуске зараженного файла, а при вызове процедуры, содержащей код передачи управления на тело вируса. Причем выполняться эта процедура может крайне редко (например, при выводе сообщения о какой-либо специфической ошибке). В результате вирус может долгие годы «спать» внутри файла и проявить себя только при некоторых ограниченных условиях.

К категории «компаньон» относятся вирусы, не изменяющие заражаемые файлы. Алгоритм работы этих вирусов состоит в том, что для заражаемого файла создается файл-двойник, причем при запуске зараженного файла управление получает именно этот двойник, то есть вирус. Наиболее распространены компаньон-вирусы, использующие особенность DOS первым выполнять файлы с расширением .COM, если в одном каталоге присутствуют два файла с одним и тем же именем, но различными расширениями имени - .COM и .EXE. Такие вирусы создают для EXE-файлов файлы-спутники, имеющие то же самое имя, но с расширением .COM, например, для файла XCOPY.EXE создается файл XCOPY.COM. Вирус записывается в COM-файл и никак не изменяет EXE-файл. При запуске такого файла DOS первым обнаружит и выполнит COM-файл, то есть вирус, который затем запустит и EXE-файл. Вторую группу составляют вирусы, которые при заражении переименовывают файл в какое-либо другое имя, запоминают его (для последующего запуска файла-хозяина) и записывают свой код на диск под именем заражаемого файла. Например, файл XCOPY.EXE переименовывается в XCOPY.EXD, а вирус записывается под именем XCOPY.EXE. При запуске управление получает код вируса, который затем запускает оригинальный XCOPY, хранящийся под именем XCOPY.EXD. Интересен тот факт, что данный метод работает, по-видимому, во всех операционных системах.

В третью группу входят так называемые "Path-companion" вирусы. Они либо записывают свой код под именем заражаемого файла, но "выше" на один уровень в прописываемых путях (DOS, таким образом, первым обнаружит и запустит файл-вирус), либо переносят файл-жертву на один подкаталог выше и т.д.

Возможно существование и других типов компаньон-вирусов, использующих иные оригинальные идеи или особенности других операционных систем.

Файловые черви (worms) являются, в некотором смысле, разновидностью компаньон-вирусов, но при этом никоим образом не связывают свое присутствие с каким-либо выполняемым файлом. При размножении они всего лишь копируют свой код в какие-либо каталоги дисков в надежде, что эти новые копии будут когда-либо запущены пользователем. Иногда эти вирусы дают своим копиям «специальные» имена, чтобы подтолкнуть пользователя на запуск своей копии - например, INSTALL.EXE или WINSTART.BAT. Существуют вирусы-черви, использующие довольно необычные приемы, например, записывающие свои копии в архивы (ARJ, ZIP и прочие). Некоторые вирусы записывают команду запуска зараженного файла в BAT-файлы. Не следует путать файловые вирусы-черви с сетевыми червями. Первые используют только файловые функции какой-либо операционной системы, вторые же при своем размножении пользуются сетевыми протоколами.

Link-вирусы, как и компаньон-вирусы, не изменяют физического содержимого файлов, однако при запуске зараженного файла «заставляют» ОС выполнить свой код. Этой цели они достигают модификацией необходимых полей файловой системы.

Вирусы, заражающие библиотеки компиляторов, объектные модули и исходные тексты программ, достаточно экзотичны и практически не распространены. Вирусы, заражающие OBJ- и LIB-файлы, записывают в них свой код в формате объектного модуля или библиотеки. Зараженный файл, таким образом, не является выполняемым и не способен на дальнейшее распространение вируса в своем текущем состоянии. Носителем же «живого» вируса становится COM- или EXE-файл.

Получив управление, файловый вирус совершает следующие общие действия:

- проверяет оперативную память на наличие своей копии и инфицирует память компьютера, если копия вируса не найдена (в случае, если вирус является резидентным), ищет незараженные файлы в текущем и (или) корневом каталоге путем сканирования дерева

каталогов логических дисков, а затем заражает обнаруженные файлы;

- выполняет дополнительные (если они есть) функции: деструктивные действия, графические или звуковые эффекты и т.д. (дополнительные функции резидентного вируса могут вызываться спустя некоторое время после активизации в зависимости от текущего времени, конфигурации системы, внутренних счетчиков вируса или других условий, в этом случае вирус при активизации обрабатывает состояние системных часов, устанавливает свои счетчики и т.д.);
- возвращает управление основной программе (если она есть). Паразитические вирусы при этом либо лечат файл, выполняют его, а затем снова заражают, либо восстанавливают программу (но не файл) в исходном виде (например, у COM-программы восстанавливается несколько первых байт, у EXE-программы вычисляется истинный стартовый адрес, у драйвера восстанавливаются значения адресов программ стратегии и прерывания).

Необходимо отметить, что чем быстрее распространяется вирус, тем вероятнее возникновение эпидемии этого вируса, чем медленнее распространяется вирус, тем сложнее его обнаружить (если, конечно же, этот вирус неизвестен). Нерезидентные вирусы часто являются "медленными" - большинство из них при запуске заражает один или два-три файла и не успевает заполонить компьютер до запуска антивирусной программы (или появления новой версии антивируса, настроенной на данный вирус). Существуют, конечно же, нерезидентные "быстрые" вирусы, которые при запуске ищут и заражают все выполняемые файлы, однако такие вирусы очень заметны: при запуске каждого зараженного файла компьютер некоторое (иногда достаточно долгое) время активно работает с винчестером, что демаскирует вирус. Скорость распространения (инфицирования) у резидентных вирусов обычно выше, чем у нерезидентных - они заражают файлы при каких-либо обращениях к ним. В результате на диске оказываются зараженными все или почти все файлы, которые постоянно используются в работе. Скорость распространения (инфицирования) резидентных файловых вирусов, заражающих файлы только при их запуске на выполнение, будет ниже, чем у вирусов, заражающих файлы и при их открытии, переименовании, изменении атрибутов файла и т.д.

Таким образом, основные деструктивные действия, выполняемые файловыми вирусами, связаны с поражением файлов (чаще исполняемых или файлов данных), несанкционированным запуском различных команд (в том числе, команд форматирования, уничтожения, копирования и т.п.), изменением таблицы векторов прерываний и др. Вместе с тем, могут выполняться и многие деструктивные действия, сходные с теми, которые указывались для загрузочных вирусов.

Макровирусы (macro viruses) являются программами на языках (макроязыках), встроенных в некоторые системы обработки данных (текстовые редакторы, электронные таблицы и т.д.). Для своего размножения такие вирусы используют возможности макроязыков и при их помощи переносят себя из одного зараженного файла (документа или таблицы) в другие. Наибольшее распространение получили макровирусы для пакета прикладных программ Microsoft Office.

Для существования вирусов в конкретной системе (редакторе) необходимо наличие встроенного в систему макроязыка с возможностями:

1) привязки программы на макроязыке к конкретному файлу;

2) копирования макропрограмм из одного файла в другой;

3) получения управления макропрограммой без вмешательства пользователя (автоматические или стандартные макросы).

Данным условиям удовлетворяют прикладные программы Microsoft Word, Excel и Microsoft Access. Они содержат в себе макроязыки: Word Basic, Visual Basic for Applications. При этом:

1) макропрограммы привязаны к конкретному файлу или находятся внутри файла;

2) макроязык позволяет копировать файлы или перемещать макропрограммы в служебные файлы системы и редактируемые файлы;

3) при работе с файлом при определенных условиях (открытие, закрытие и т.д.) вызываются макропрограммы (если таковые есть), которые определены специальным образом или имеют стандартные имена.

Данная особенность макроязыков предназначена для автоматической обработки данных в больших организациях или в глобальных сетях и позволяет организовать так называемый "автоматизированный документооборот". С другой стороны, возможности макроязыков таких систем позволяют вирусу переносить свой код в другие файлы и таким образом заражать их.

Большинство макровирусов активны не только в момент открытия (закрытия) файла, но до тех пор, пока активен сам редактор. Они содержат все свои функции в виде стандартных макросов Word/Excel/Office. Существуют, однако, вирусы, использующие приемы скрытия своего кода и хранящие свой код в виде не макросов. Известно три подобных приема, все они используют возможность макросов создавать, редактировать и исполнять другие макросы. Как правило, подобные вирусы имеют небольшой (иногда - полиморфный) макрос-загрузчик вируса, который вызывает встроенный редактор макросов, создает новый макрос, заполняет его основным кодом вируса, выполняет и затем, как правило, уничтожает (чтобы скрыть следы присутствия вируса). Основной код таких вирусов присутствует либо в самом макросе вируса в виде текстовых строк (иногда - зашифрованных), либо хранится в области переменных документа.

К сетевым относятся вирусы, которые для своего распространения активно используют протоколы и возможности локальных и глобальных сетей. Основным принципом работы сетевого вируса является возможность самостоятельно передать свой код на удаленный сервер или рабочую станцию. "Полноценные" сетевые вирусы при этом обладают еще и возможностью запустить на выполнение свой код на удаленном компьютере или, по крайней мере, "подтолкнуть" пользователя к запуску зараженного файла.

Вредоносными программами, обеспечивающими осуществление НСД, могут быть:

- программы подбора и вскрытия паролей;
- программы, реализующие угрозы;
- программы, демонстрирующие использование недекларированных возможностей программного и программно-аппаратного обеспечения ИСПДн;
- программы-генераторы компьютерных вирусов;
- программы, демонстрирующие уязвимости средств защиты информации и др.

В связи с усложнением и возрастанием разнообразия программного обеспечения число вредоносных программ быстро возрастает. Сегодня известно более 120 тысяч сигнатур компьютерных вирусов. Вместе с тем, далеко не все из них представляют реальную угрозу. Во многих случаях устранение уязвимостей в системном или прикладном программном обеспечении привело к тому, что ряд вредоносных программ уже не способен внедриться в них. Часто основную опасность представляют новые вредоносные программы.

5.6. Общая характеристика нетрадиционных информационных каналов

Нетрадиционный информационный канал - это канал скрытной передачи информации с использованием традиционных каналов связи и специальных преобразований передаваемой информации, не относящихся к криптографическим.

Для формирования нетрадиционных каналов могут использоваться методы:

- компьютерной стеганографии;
- основанные на манипуляции различных характеристик ИСПДн, которые можно получать санкционировано (например, времени обработки различных запросов, объемов доступной памяти или доступных для чтения идентификаторов файлов или процессов и т.п.).

Методы компьютерной стеганографии предназначены для скрытия факта передачи сообщения путем встраивания скрываемой информации во внешне безобидные данные

(текстовые, графические, аудио- или видеофайлы) и включают в себя две группы методов, основанных:

- на использовании специальных свойств компьютерных форматов хранения и передачи данных;
- на избыточности аудио-, визуальной или текстовой информации с позиции психофизиологических особенностей восприятия человека.

Классификация методов компьютерной стеганографии приведена на рисунке 15. Их сравнительная характеристика приведена в таблице 4.

Наибольшее развитие и применение в настоящее время находят методы сокрытия информации в графических стегоконтейнерах. Это обусловлено сравнительно большим объемом информации, который можно разместить в таких контейнерах без заметного искажения изображения, наличием априорных сведений о размерах контейнера, существованием в большинстве реальных изображений текстурных областей, имеющих шумовую структуру и хорошо подходящих для встраивания информации, проработанностью методов цифровой обработки изображений и цифровых фор матов представления изображений. В настоящее время существует целый ряд как коммерческих, так и бесплатных программных продуктов, доступных обычному пользователю, реализующих известные стеганографические методы сокрытия информации. При этом преимущественно используются графические и аудио-контейнеры.

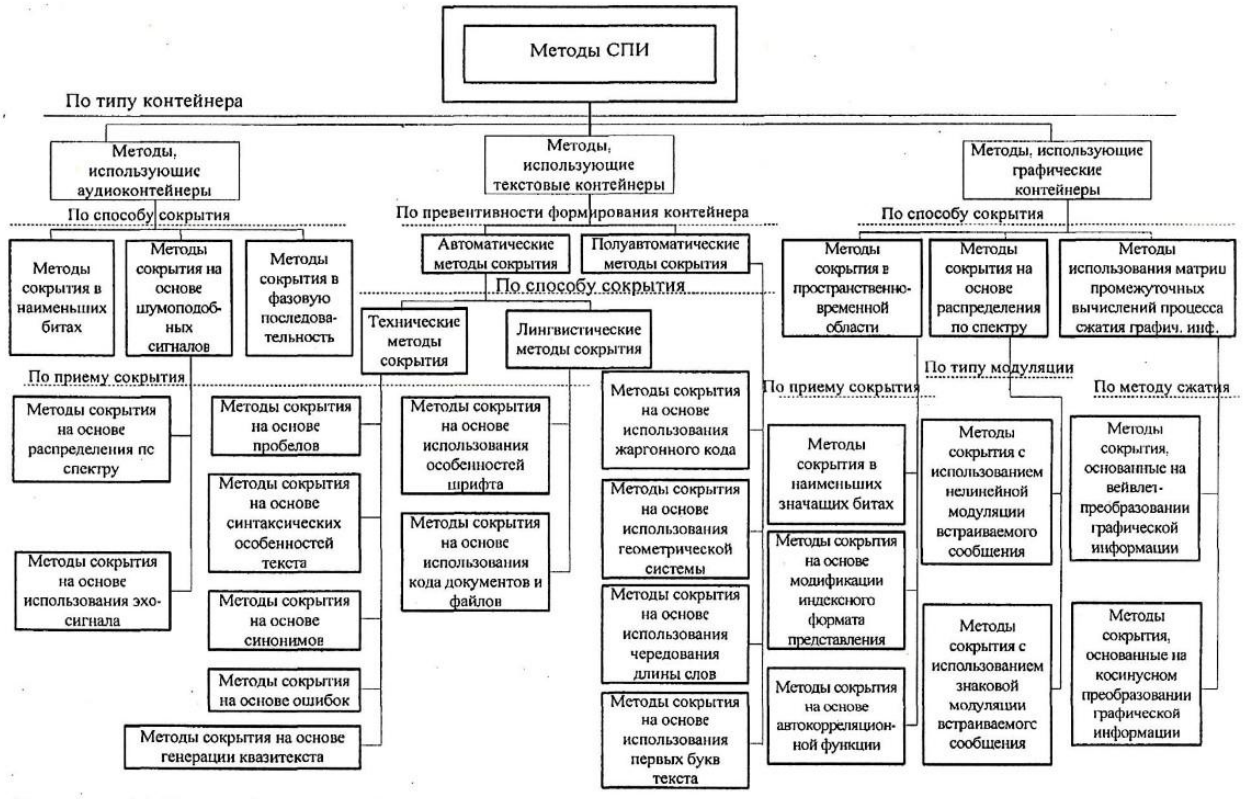


Рисунок 15. Классификация методов стеганографического преобразования информации (СПИ)

Таблица 4

Сравнительная характеристика стеганографических методов преобразования информации

Стеганографический метод	Краткая характеристика метода	Недостатки	Преимущества
Методы сокрытия информации в аудиоконтейнерах			

Метод сокрытия в наименьших значащих битах	Основан на записи сообщения в наименьшие значащие биты исходного сигнала. В качестве контейнера используется, как правило, несжатый аудиосигнал	Невысокая скрытность передачи сообщения. Низкая устойчивость к искажениям. Используется только для определенных форматов аудио-файлов	Достаточно высокая емкость контейнера (до 25%)
Метод сокрытия на основе распределения по спектру	Основан на генерации псевдослучайного шума, являющегося функцией внедряемого сообщения, и подмешивании полученного шума к основному сигналу-контейнеру в качестве аддитивной составляющей. Кодирование потоков информации путем рассеяния кодированных данных по спектру частот	Низкий коэффициент использования контейнера. Значительные вычислительные затраты	Сравнительно высокая скрытность сообщения
Метод сокрытия на основе использования эхо-сигнала	Основан на использовании в качестве шумоподобного сигнала самого аудиосигнала, задержанного на различные периоды времени в зависимости от внедряемого сообщения ("дозвоночного эха")	Низкий коэффициент использования контейнера. Значительные вычислительные затраты	Сравнительно высокая скрытность сообщения
Метод сокрытия в фазе сигнала	Основан на факте нечувствительности уха человека к абсолютному значению фазы гармоник. Аудио-сигнал разбивается на последовательность сегментов, сообщение встраивается путем модификации фазы первого сегмента	Малый коэффициент использования контейнера	Обладает значительно более высокой скрытностью, чем методы сокрытия в НЗБ
Методы сокрытия информации в текстовых контейнерах			
Метод сокрытия на основе пробелов	Основан на вставке пробелов в конце	Методы чувствительны к переносу	Достаточно большая пропускная

	строчек, после знаков препинания, между словами при выравнивании длины строк	текста из одного формата в другой. Возможна потеря сообщения. Невысокая скрытность	способность
Метод сокрытия на основе синтаксических особенностей текста	Основан на том, что правила пунктуации допускают неоднозначности при расстановке знаков препинания	Очень низкая пропускная способность. Сложность детектирования сообщения	Существует потенциальная возможность подобрать такой метод, при котором потребуются весьма сложные процедуры для раскрытия сообщения
Метод сокрытия на основе синонимов	Основан на вставке информации в текст при помощи чередования слов из какой-либо группы синонимов	Сложен применительно к русскому языку в связи с большим разнообразием оттенков в разных синонимах	Один из наиболее перспективных методов. Обладает сравнительно высокой скрытностью сообщения
Метод сокрытия на основе использования ошибок	Основан на маскировке информационных битов под естественные ошибки, опечатки, нарушения правил написания сочетаний гласных и согласных, замене кириллицы на аналогичные по внешнему виду латинские буквы и др.	Невысокая пропускная способность. Быстро вскрывается при статистическом анализе.	Весьма прост в применении. Высокая скрытность при анализе человеком
Метод сокрытия на основе генерации квазитекста	Основан на генерации текстового контейнера с использованием набора правил построения предложений. Используется симметричная криптография	Невысокая пропускная способность. Бессмысленность созданного текста	Скрытность определяется методами шифрования и, как правило, весьма высока
Метод сокрытия на основе использования особенностей шрифта	Основан на вставке информации за счет изменения типа шрифта и размера букв, а также на возможности встраивания информации в блоки с неизвестными для браузера идентификаторами	Легко выявляется при преобразовании масштаба документа, при статистическом стегоанализе	Высокий коэффициент использования контейнера
Метод сокрытия на	Основан на	Низкая скрытность	Прост в применении

основе использования кода документа и файла	размещении информации в зарезервированных и неиспользуемых полях переменной длины	при известном формате файла	
Метод сокрытия на основе использования жаргона	Основан на изменении значений слов	Низкая пропускная способность. Узко специализирован. Низкая скрытность	Прост в применении
Метод сокрытия на основе использования чередования длины слов	Основан на генерации текста - контейнера с формированием слов определенной длины по известному правилу кодирования	Сложность формирования контейнера и сообщения	Достаточно высокая скрытность при анализе человеком
Метод сокрытия на основе использования первых букв	Основан на внедрении сообщения в первые буквы слов текста с подбором слов	Сложность составления сообщения. Низкая скрытность сообщения	Дает большую свободу выбора оператору, придумывающему сообщение
Методы сокрытия информации в графических контейнерах			
Метод сокрытия в наименьших значащих битах	Основан на записи сообщения в наименьшие значащие биты исходного изображения	Невысокая скрытность передачи сообщения. Низкая устойчивость к искажениям	Достаточно высокая емкость контейнера (до 25%)
Метод сокрытия на основе модификации индексного формата представления	Основан на редукции (замене) цветовой палитры и упорядочивании цветов в пикселях с соседними номерами	Применяется преимущественно к сжатым изображениям. Невысокая скрытность передачи сообщения	Сравнительно высокая емкость контейнера
Метод сокрытия на основе использования автокорреляционной функции	Основан на поиске с применением автокорреляционной функции областей, содержащих сходные данные	Сложность расчетов	Устойчивость к большинству нелинейных преобразований контейнера
Метод сокрытия на основе использования нелинейной модуляции встраиваемого сообщения	Основан на модуляции псевдослучайного сигнала сигналом, содержащим скрываемую информацию	Низкая точность детектирования. Искажения	Достаточно высокая скрытность сообщения
Метод сокрытия на основе использования знаковой модуляции встраиваемого сообщения	Основан на модуляции псевдослучайного сигнала биполярным сигналом, содержащим скрываемую	Низкая точность детектирования. Искажения	Достаточно высокая скрытность сообщения

	информацию		
Метод сокрытия на основе вейвлет-преобразования	Основан на особенностях вейвлет-преобразований	Сложность расчетов	Высокая скрытность
Метод сокрытия на основе использования дискретного косинусного преобразования	Основан на особенностях дискретного косинусного преобразования	Сложность расчетов	Высокая скрытность

В нетрадиционных информационных каналах, основанных на манипуляции различных характеристик ресурсов ИСПДн, используются для передачи данных некоторые разделяемые ресурсы. При этом в каналах, использующих временные характеристики, осуществляется модуляция по времени занятости разделяемого ресурса (например, модулируя время занятости процессора, приложения могут обмениваться данными).

В каналах памяти ресурс используется как промежуточный буфер (например, приложения могут обмениваться данными путем помещения их в имена создаваемых файлов и директорий). В каналах баз данных и знаний используют зависимости между данными, возникающими в реляционных базах данных и знаний.

Нетрадиционные информационные каналы могут быть сформированы на различных уровнях функционирования ИСПДн:

- на аппаратном уровне;
- на уровне микрокодов и драйверов устройств;
- на уровне операционной системы;
- на уровне прикладного программного обеспечения;
- на уровне функционирования каналов передачи данных и линий связи.

Эти каналы могут использоваться как для скрытой передачи скопированной информации, так и для скрытной передачи команд на выполнение деструктивных действий, запуска приложений и т.п.

Для реализации каналов, как правило, необходимо внедрить в автоматизированную систему программную или программно-аппаратную закладку, обеспечивающую формирование нетрадиционного канала.

Нетрадиционный информационный канал может существовать в системе непрерывно или активизироваться одноразово или по заданным условиям. При этом возможно существование обратной связи с субъектом НСД.

5.7. Общая характеристика результатов несанкционированного или случайного доступа

Реализация угроз НСД к информации может приводить к следующим видам нарушения ее безопасности:

- нарушению конфиденциальности (копирование, неправомерное распространение);
- нарушению целостности (уничтожение, изменение);
- нарушению доступности (блокирование).
- Нарушение конфиденциальности может быть осуществлено в случае утечки информации:
- копирования ее на отчуждаемые носители информации;
- передачи ее по каналам передачи данных;
- при просмотре или копировании ее в ходе ремонта, модификации и утилизации программно-аппаратных средств;
- при «сборке мусора» нарушителем в процессе эксплуатации ИСПДн.

Нарушение целостности информации осуществляется за счет воздействия (модификации) на программы и данные пользователя, а также технологическую (системную) информацию, включающую:

- микропрограммы, данные и драйвера устройств вычислительной системы;
- программы, данные и драйвера устройств, обеспечивающих загрузку операционной системы;
- программы и данные (дескрипторы, описатели, структуры, таблицы и т.д.) операционной системы;
- программы и данные прикладного программного обеспечения;
- программы и данные специального программного обеспечения;
- промежуточные (оперативные) значения программ и данных в процессе их обработки (чтения/записи, приема/передачи) средствами и устройствами вычислительной техники.

Нарушение целостности информации в ИСПДн может также быть вызвано внедрением в нее вредоносной программы программно-аппаратной закладки или воздействием на систему защиты информации или ее элементы.

Кроме этого, в ИСПДн возможно воздействие на технологическую сетевую информацию, которая может обеспечивать функционирование различных средств управления вычислительной сетью:

- конфигурацией сети;
- адресами и маршрутизацией передачи данных в сети;
- функциональным контролем сети;
- безопасностью информации в сети.

Нарушение доступности информации обеспечивается путем формирования (модификации) исходных данных, которые при обработке вызывают неправильное функционирование, отказы аппаратуры или захват (загрузку) вычислительных ресурсов системы, которые необходимы для выполнения программ и работы аппаратуры.

Указанные действия могут привести к нарушению или отказу функционирования практически любых технических средств ИСПДн:

- средств обработки информации;
- средств ввода/вывода информации;
- средств хранения информации;
- аппаратуры и каналов передачи;
- средств защиты информации.

6. Отнесение к классу (виду) информационных систем персональных данных, используемых в ГБУ «ИГТК»

В зависимости от целей и содержания обработки ПДн оператор может осуществлять обработку ПДн в ИСПДн различных типов.

По структуре информационные системы подразделяются на автоматизированные рабочие места, локальные информационные системы и распределенные информационные системы.

По наличию подключений к сетям связи общего пользования и (или) сетям международного информационного обмена информационные системы подразделяются на системы, имеющие подключения, и системы, не имеющие подключений.

По режиму обработки персональных данных в информационной системе информационные системы подразделяются на однопользовательские и многопользовательские.

По разграничению прав доступа пользователей информационные системы подразделяются на системы без разграничения прав доступа и системы с разграничением прав доступа.

Информационные системы в зависимости от местонахождения их технических средств подразделяются на системы, все технические средства которых находятся в пределах Российской Федерации, и системы, технические средства которых частично или целиком находятся за пределами Российской Федерации.

В зависимости от технологий, состава и характеристик технических средств ИСПДн, а также опасности реализации УБПДн и наступления последствий в результате несанкционированного или случайного доступа можно выделит следующие типы ИСПДн:

- автоматизированные рабочие места, не имеющие подключение к сетям связи общего пользования и (или) сетям международного информационного обмена;
- автоматизированные рабочие места, имеющие подключение к сетям связи общего пользования и (или) сетям международного информационного обмена;
- локальные ИСПДн, не имеющие подключение к сетям связи общего пользования и (или) сетям международного информационного обмена;
- локальные ИСПДн, имеющие подключение к сетям связи общего пользования и (или) сетям международного информационного обмена;
- распределенные ИСПДн, не имеющие подключение к сетям связи общего пользования и (или) сетям международного информационного обмена;
- распределенные ИСПДн, имеющие подключение к сетям связи общего пользования и (или) сетям международного информационного обмена.

В ГБУ «ИГТК» используется распределённая информационная система обработки персональных данных, подключённая к сетям связи общего пользования.

6.1. Типовая модель угроз безопасности персональных данных, обрабатываемых в распределенных информационных системах персональных данных, имеющих подключение к сетям связи общего пользования и (или) сетям международного информационного обмена

При обработке ПДн в распределенных ИСПДн, имеющих подключение к сетям связи общего пользования и (или) сетям международного информационного обмена, возможна реализация следующих УБПДн:

- угрозы утечки информации по техническим каналам;
- угрозы НСД к ПДн, обрабатываемым на автоматизированном рабочем месте.
- Угрозы утечки информации по техническим каналам включают в себя:
- угрозы утечки видовой информации;
- угрозы утечки информации по каналу ПЭМИН.

В связи с отсутствием функций голосового ввода ПДН и воспроизведения ПДН акустическими средствами в используемых в ГБУ «ИГТК» ИСПДН угроза утечки акустической информации, содержащейся в ИСПДН, не возникает.

Возникновение УБПДн в рассматриваемых ИСПДн по техническим каналам характеризуется теми же условиями и факторами, которыми данные угрозы характеризуются обработка персональных данных в автоматизированных рабочих местах, не имеющих подключения к сетям связи общего пользования и (или) сетям международного информационного обмена; автоматизированных рабочих местах, имеющих подключение к сетям связи общего пользования и (или) сетям международного информационного обмена; в локальных информационных системах персональных данных, не имеющих подключения к сетям связи общего пользования и (или) сетям международного информационного обмена; в локальных информационных системах персональных данных, имеющих подключение к сетям связи общего пользования и (или) сетям международного информационного обмена; в распределённых информационных системах персональных данных, не имеющих подключения к сетям связи общего пользования и (или) к сетям международного информационного обмена.

Угрозы НСД связаны с действиями нарушителей, имеющих доступ к ИСПДн, включая пользователей ИСПДн, реализующих угрозы непосредственно в ИСПДн, а также

нарушителей, не имеющих доступа к ИСПДн, реализующих угрозы из внешних сетей связи общего пользования и (или) сетей международного информационного обмена.

Угрозы НСД, связанные с действиями нарушителей, имеющих доступ к ИСПДн, аналогичны тем, которые имеют место в распределенных ИСПДн, не имеющей подключения к сетям общего пользования. Кроме того, в такой ИСПДн имеют место угрозы, реализуемые с использованием протоколов межсетевого взаимодействия из внешних сетей, в том числе:

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