УТВЕРЖДАЮ

Председатель
Комитета по образованию

О.В.Иванова

«_____» _____2011 г.

м.п.

Частная модель угроз
безопасности персональных данных
при их обработке в ИСПДн
«Управление персоналом государственных органов»

СОГЛАСОВАНО

Начальник отдела государственной службы и организационно-правовой работы

_____В.В.Литвинова

«_____» _____2011 г.

РАЗРАБОТАЛ

Старший инженер отдела государственной службы и организационно-правовой работы

_____С.В.Литовский

«_____» _____2011 г.

СОГЛАСОВАНО

Ведущий специалист отдела государственной службы и организационно-правовой работы

_____С.И.Яицкий

«_____» _____2011 г.

2011 г.

Содержание

Сокращения, условные обозначения

АРМ – автоматизированное рабочее место
ВТСС – вспомогательные технические средства и системы
ИСПДн – информационная система персональных данных
КЗ – контролируемая зона
НДВ – не декларированные возможности
НСД – несанкционированный доступ
ОБПДн – обеспечение безопасности персональных данных
ОС – операционная система
ПДн – персональные данные
ПМВ – программно-математическое воздействие
ПЭМИН – побочные электромагнитные излучения и наводки
ТКУИ – технические каналы утечки информации
УБПДн – угрозы безопасности персональных данных

Термины и 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 инфор-

мации (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 распространение 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.

Не декларированные 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, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных.

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, организующее и (или) осуществляющее обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

Технические средства информационной системы персональных данных – 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), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации).

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, год, месяц, 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 – код программы, преднамеренно внесенный в программу с целью осуществить утечку, изменить, блокировать, уничтожить информацию или уничтожить и модифицировать программное обеспечение объекта информатизации и (или) блокировать аппаратные средства.

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.

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 которого 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 - способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

Введение

Современная система обеспечения информационной безопасности должна строиться на основе комплексирования разнообразных мер защиты и должна опираться на современные методы прогнозирования, анализа и моделирования возможных угроз безопасности информации и последствий их реализации.

Результаты моделирования предназначены для выбора адекватных оптимальных методов парирования угроз.

На стадии моделирования проведено изучение и анализ существующей обстановки и выявлены актуальные угрозы безопасности ПДн в составе ИСПДн «Управление персоналом государственных органов».

Модель угроз построена в соответствии с требованиями Федерального Закона от 27.07.2006 г. № 152-ФЗ «О персональных данных» и методическими документами ФСТЭК России:

- «Базовая модель угроз безопасности ПДн при их обработке в ИСПДн»;
- «Методика определения актуальных угроз безопасности ПДн при их обработке в ИСПДн».

1. Описание подхода к моделированию угроз безопасности ПДн.

Модель угроз безопасности ПДн в составе ИСПДн «Управление персоналом государственных органов» разработана на основе методических документов ФСТЭК:

- «Базовая модель угроз безопасности ПДн при их обработке в ИСПДн»;
- «Методика определения актуальных угроз безопасности ПДн при их обработке в ИСПДн».

«Базовая модель угроз безопасности ПДн при их обработке в ИСПДн» содержит систематизированный перечень угроз безопасности ПДн при их обработке в ИСПДн, обусловленных преднамеренными или непреднамеренными действиями физических лиц, действиями зарубежных спецслужб или организаций, а также криминальных группировок, создающими условия для нарушения безопасности ПДн.

На основе «Базовой модели угроз безопасности ПДн при их обработке в ИСПДн» проведена классификация угроз безопасности ПДн в составе ИСПДн «Управление персоналом государственных органов»

и составлен перечень угроз безопасности ПДн в составе ИСПДн.

На основе составленного перечня угроз безопасности ПДн в составе ИСПДн с помощью «Методики определения актуальных угроз безопасности ПДн при их обработке в ИСПДн» построена модель угроз безопасности ПДн в составе ИСПДн «Управление персоналом государственных органов» и выявлены актуальные угрозы.

2. Классификация угроз безопасности персональных данных в ИСПДн АСУ «Управление персоналом государственных органов».

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 угроз.

К характеристикам ИСПДн, обуславливающим 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 ПДн, режимы разграничения прав доступа пользователей ИСПДн, местонахождение и условия размещения технических средств ИСПДн.

ИСПДн «Управление персоналом государственных органов» представляет собой совокупность информационных и программно-аппаратных элементов и их особенностей как объектов обеспечения безопасности.

Основными элементами ИСПДн являются:

- персональные данные, содержащиеся в базах данных ИСПДн «Управление персоналом государственных органов»;
- информационные технологии, как совокупность приемов, способов и методов применения средств вычислительной техники при обработке ПДн;
- технические средства, осуществляющие обработку ПДн;
- программные средства (операционные системы, системы управления базами данных и т.п.);
- средства защиты информации;
- вспомогательные технические средства и системы.

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

Возможности источников УБПДн обусловлены совокупностью методов и 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 необходимые условия для нарушения безопасности ПДн (несанкционированный или случайный доступ).

Основными **элементами канала реализации** УБПДн 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 находит свое отражение в виде символов, обра-

зов, сигналов, технических решений и процессов, количественных характеристик физических величин.

Носители ПДн могут содержать информацию, представленную в следующих видах:

- акустическая (речевая) информация, содержащаяся непосредственно в произносимой речи пользователя ИСПДн при осуществлении им функции голосового ввода ПДн в ИСПДн, а также содержащаяся в электромагнитных полях и электрических сигналах, которые возникают за счет преобразований акустической информации;
- видовая информация, 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, IP-протоколов, файлов и других логических структур.

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

1. по видам возможных источников УБПДн;

– угрозы, связанные с преднамеренными или непреднамеренными действиями лиц, имеющими доступ к ИСПДн, включая пользователей ИСПДн, реализующие угрозы непосредственно в ИСПДн (внутренний нарушитель);

– угрозы, связанные с преднамеренными или непреднамеренными действиями лиц, не имеющих доступа к ИСПДн, реализующие угрозы из внешних сетей связи общего пользования и (или) сетей международного информационного обмена (внешний нарушитель).

2. по структуре ИСПДн, на которую направлена реализация УБПДн;

– угрозы безопасности ПДн, обрабатываемых в ИСПДн на базе автоматизированного рабочего места;

– угрозы безопасности ПДн, обрабатываемых в ИСПДн на базе локальных информационных систем;

– угрозы безопасности ПДн, обрабатываемых в ИСПДн на базе распределенных информационных систем.

3. по виду несанкционированных действий, осуществляемых с ПДн;

– 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.

4. по способам реализации УБПДн;

– угрозы, реализуемые в ИСПДн при их подключении к сетям связи общего пользования;

– угрозы, реализуемые в ИСПДн при их подключении к сетям международного информационного обмена;

– угрозы, реализуемые в ИСПДн не имеющих подключений к сетям связи общего пользования и сетям международного информационного обмена.

5. по виду каналов, с использованием которых реализуется УБПДн.

– угрозы, реализуемые через каналы, возникающие за счет использования технических средств съема (добывания) информации, обрабатываемой в технических средствах ИСПДн или ВТСС (технические каналы утечки информации);

– угрозы, реализуемые за счет несанкционированного доступа к ПДн в ИСПДн с использованием штатного программного обеспечения ИСПДн или специально разрабатываемого программного обеспечения.

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

- значительные негативные последствия для субъектов ПДн;
- негативные последствия для субъектов ПДн;
- незначительные негативные последствия 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 и описываются следующим образом:

угроза утечки ПДн по техническим каналам: *= <источник угрозы (приемник информативного сигнала)>, <среда (путь) распространения информационного сигнала>, <источник (носитель) ПДн>.*

Угрозы, связанные с НСД, представляются в виде совокупности обобщенных классов возможных источников угроз НСД, уязвимостей программного и аппаратного обеспечения ИСПДн, способов реализации угроз, объектов воздействия (носителей защищаемой информации) и возможных деструктивных действий. Такое представление описывается следующей формализованной записью:

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

3. Общее описание угроз безопасности персональных данных обрабатываемых в ИСПДн АСУ «Управление персоналом государственных органов»

При обработке ПДн в ИСПДн «Управление персоналом государственных органов» возможна реализация следующих видов УБПДн:

– угрозы утечки информации по техническим каналам;

– угрозы НСД к ПДн, обрабатываемым в ИСПДн.

3.1. Угрозы утечки информации по техническим каналам.

Основными элементами угроз утечки информации по техническим каналам являются:

1. источник угрозы (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 регистрации, приема или фотографирования информации);

2. среда (путь) распространения информативного сигнала (физическая среда, по которой информативный сигнал может распространяться и приниматься (регистрироваться) приемником);

3. носитель защищаемой информации (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 возможно возникновение УБПДн за счет реализации следующих технических каналов утечки информации:

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

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

Реализация угрозы утечки видовой информации возможна за счет просмотра информации 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.

Угрозы утечки информации по каналу ПЭМИН, возможны из-за наличия электромагнитных излучений, в основном, монитора и системного блока компьютера. Основную опасность представляют угрозы утечки из-за наличия электромагнитных излучений монитора.

3.2. Угрозы несанкционированного доступа.

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 (копирования, несанкционированного распространения), целостности (уничтожения, изменения) и доступности (блокирования) ПДн, и включают в себя:

1. Угрозы доступа (проникновения) в операционную среду компьютера с использованием штатного программного обеспечения;

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.

2. *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 создания нештатных режимов работы программных (программно-аппаратных) средств - это угрозы «Отказа в обслуживании». 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.

3. *Угрозы внедрения вредоносных программ* (программно-математического воздействия).

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).

4. Модель угроз безопасности персональных данных обрабатываемых в ИСПДн «Управление персоналом государственных органов».

В соответствии с разделом 5 при обработке ПДн в ИСПДн АСУ «Управление персоналом государственных органов», возможна реализация следующих видов УБПДн:

- угрозы утечки информации по техническим каналам;
- угрозы НСД к ПДн, обрабатываемым в ИСПДн;

4.1. Угрозы утечки информации по техническим каналам.

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

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

4.1.1. 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.

Утечка акустической (речевой) информации может быть осуществлена:

– с помощью аппаратных закладок;

– за счет съема виброакустических сигналов;

– за счет излучений модулированных акустическим сигналом (микрофонный эффект и ВЧ облучение).

В ИСПДн «Управление персоналом государственных органов» *не реализованы функции голосового ввода ПДн в ИСПДн. Акустические средства воспроизведения ПДн в ИСПДн* «Управление персоналом государственных органов» *не предусмотрены.*

Рассмотрение угроз утечки акустической (речевой) информации не целесообразно в связи с отсутствием предпосылок возникновения угроз.

4.1.2. 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.

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

Утечка видовой информации может быть осуществлена:

– за счет удаленного просмотра экранов дисплеев и других средств отображения информации;

– с помощью видео аппаратных закладок

В ИСПДн «Управление персоналом государственных органов» *отсутствует возможность неконтролируемого пребывания физических лиц в служебных помещениях или в непосредственной близости от них, соответственно отсутствует возможность непосредственного наблюдения посторонними лицами ПДн.*

Рассмотрение угроз утечки видовой информации не целесообразно в связи с отсутствием предпосылок возникновения угроз.

4.1.3. Угрозы утечки информации по каналам ПЭМИН.

Возникновение угрозы ПДн по каналам ПЭМИН возможно за счет перехвата техническими средствами побочных информативных электромагнитных полей и электрических сигналов, возникающих при обработке ПДн техническими средствами ИСПДн.

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

Регистрации ПЭМИН осуществляется с целью перехвата информации, циркулирующей в технических средствах, осуществляющих обработку ПДн (средствах вычислительной техники, информационно-вычислительных комплексах и

сетях, средствах и системах передачи, приема и обработки ПДн, средствах и системах звукозаписи, звукоусиления, звуковоспроизведения, переговорных и телевизионных устройствах, средствах изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации).

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

Утечка информации по каналам ПЭМИН может быть осуществлена:

- за счет побочных ЭМ излучений ЭВТ;
- за счет наводок по цепям питания;
- за счет радио излучений, модулированных информационным сигналом.

Рассмотрение угроз безопасности ПДн, связанных с перехватом ПЭМИН в ИСПДн «Управление персоналом государственных органов» избыточно, так как носители ПДн (технические средства ИСПДн, создающие физические поля, в которых информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин) находятся в пределах контролируемой зоны.

Утечка ПДн по каналам ПЭМИН – маловероятна из-за несоответствия стоимости средств съема информации и полученной в результате регистрации ПЭМИН информации, а защита ПДн от данного вида угроз – экономически нецелесообразна.

4.2. Угрозы НСД к ПДн, обрабатываемым в ИСПДн.

Угрозы НСД связаны с действиями нарушителей, имеющих доступ к ИСПДн, включая пользователей ИСПДн, реализующих угрозы непосредственно в ИСПДн. Кроме этого, источниками угроз НСД к информации в ИСПДн могут быть аппаратные закладки и отчуждаемые носители вредоносных программ.

В ИСПДн «Управление персоналом государственных органов» возможны:

1. угрозы, реализуемые в ходе загрузки операционной системы:
   - перехват паролей или идентификаторов;
   - модификация базовой системы ввода/ вывода (BIOS), перехват управления загрузкой;
2. угрозы, реализуемые после загрузки операционной системы:
   - выполнение несанкционированного доступа с применением стандартных функций операционной системы;
   - выполнение несанкционированного доступа с помощью прикладной программы (например, системы управления базами данных);
   - выполнение несанкционированного доступа с применением специально созданных для выполнения НСД программ (программ просмотра и модификации реестра, поиска текстов в текстовых файлах и т.п.);
   - утечка информации с использованием копирования ее на съемные носители;
   - утечка информации за счет ее несанкционированной передачи по каналам связи;
3. угрозы внедрения вредоносных программ с использованием съемных носителей;
4. угрозы утечки информации с помощью аппаратных закладок;
5. угрозы «Анализа сетевого трафика» - перехват передаваемой во внешние сети и принимаемой из внешних сетей информации;

6. угрозы сканирования – выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др.

7. угрозы получения НСД путем подмены доверенного объекта:

– обход системы идентификации и аутентификации сообщений;

– обход системы идентификации и аутентификации сетевых объектов.

8. угрозы внедрения ложного объекта сети – перехват запросов и модификация адресных данных (с использованием протоколов SAP, ARP, DNS, WINS)

9. угрозы навязывания ложного маршрута – несанкционированное изменение маршрутно-адресных данных (с использованием протоколов RIP, OSPF, LSP, ICMP, SNMP)

10. угрозы выявления паролей:

– перехват и взлом паролей;

– подбор паролей доступа;

11. угрозы типа «Отказ в обслуживании»;

12. угрозы удаленного запуска приложений:

– внедрение троянских программ;

– атаки типа «переполнение буфера»;

– с использованием средств удаленного управления;

13. угрозы внедрения по сети вредоносных программ:

– внедрение вредоносных программ через почтовые сообщения;

– внедрение вредоносных программ через обмен и загрузку файлов;

– внедрение вредоносных программ через зараженные web страницы;

– заражение сетевыми червями, использующими уязвимости сетевого ПО.

4.2.1. Общая характеристика источников угроз НСД.

Источниками угроз НСД в ИСПДн могут быть:

1. нарушитель;
2. носитель вредоносной программы;
3. аппаратная закладка.

4.2.1.1. Нарушитель

По наличию права постоянного или разового доступа в ИСПДн нарушители подразделяются на два типа:

1. ***Внешние нарушители*** - нарушители, не имеющие доступа к ИСПДн, реализующие угрозы из внешних сетей связи общего пользования и (или) сетей международного информационного обмена;

2. ***Внутренние нарушители*** - нарушители, имеющие доступ к ИСПДн, включая пользователей ИСПДн, реализующие угрозы непосредственно в ИСПДн.

Так как ИСПДн «Управление персоналом государственных органов» является распределенной ИСПДн, не имеющей подключений к сетям общего пользования и (или) сетям международного обмена, внешний нарушитель не рассматривается.

Внутренние потенциальные нарушители подразделяются на **восемь категорий** в зависимости от способа доступа и полномочий доступа к ПДн (Таблица 1).

Таблица 1

Категории нарушителей

Категория нарушителя	Способ доступа и полномочия
K_1	Лица, имеющие санкционированный доступ к ИСПДн, но не имеющие доступа к ПДн. К этому типу нарушителей относятся должностные лица, обеспечивающие нормальное функционирование ИСПДн
K_2	Зарегистрированные пользователи ИСПДн, осуществляющие ограниченный доступ к ресурсам ИСПДн с рабочего места
K_3	Зарегистрированные пользователи ИСПДн, осуществляющие удаленный доступ к ПДн по локальным и (или) распределенным информационным системам
K_4	Зарегистрированные пользователи ИСПДн с полномочиями администратора безопасности сегмента (фрагмента) ИСПДн
K_5	Зарегистрированные пользователи с полномочиями системного администратора ИСПДн
K_6	Зарегистрированные пользователи с полномочиями администратора безопасности ИСПДн
K_7	Программисты-разработчики (поставщики) прикладного программного обеспечения и лица, обеспечивающие его сопровождение на защищаемом объекте
K_8	Разработчики и лица, обеспечивающие поставку, сопровождение и ремонт технических средств на ИСПДн

4.2.1.2. Носитель вредоносной программы

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:

1. отчуждаемый носитель, то есть дискета, оптический диск (CD-R, CD-RW), флэш-память, отчуждаемый винчестер и т.п.;

2. 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;

3. 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:

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

4.2.1.3. Аппаратная закладка

В ИСПДн имеется опасность применения аппаратных средств, предназначенных для регистрации вводимой с клавиатуры информации, например:

- аппаратная закладка внутри клавиатуры;
- считывание данных с кабеля клавиатуры бесконтактным методом;
- включение устройства в разрыв кабеля;
- аппаратная закладка внутри системного блока и др.

В ИСПДн АСУ «Управление персоналом государственных органов» *отсутствует возможность неконтролируемого пребывания физических лиц в служебных помещениях или в непосредственной близости от них, соответственно отсутствует возможность установки аппаратных закладок посторонними лицами.*

Существование данного источника угроз маловероятно также из-за несоответствия стоимости аппаратных закладок, сложности их скрытой установки и полученной в результате информации.

4.2.2. Общая характеристика уязвимостей ИСПДн.

Уязвимость ИСПДн – недостаток или слабое место в системном или прикладном программном (программно-аппаратном) обеспечении автоматизированной информационной системы, которое может быть использовано для реализации угрозы безопасности персональных данным.

Причины возникновения уязвимостей:

- 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;
- несанкационированные 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.).

К основным группам уязвимостей ИСПДн, относятся:

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

4.2.2.1. Характеристика уязвимостей системного ПО.

Уязвимости системного программного обеспечения необходимо рассматривать с привязкой к архитектуре построения вычислительных систем. При этом возможны уязвимости:

1. в микропрограммах, в прошивках запоминающих устройств;
2. 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;
3. 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.);
4. 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.

4.2.2.2. Характеристика уязвимостей прикладного ПО.

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

Прикладные программы общего пользования – текстовые и графические редакторы, медиа-программы (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 использования 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.

4.2.3. Характеристика угроз непосредственного доступа в операционную среду ИСПДн

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 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), обусловленной 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:

1. Угрозы, реализуемые в ходе загрузки операционной системы

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

Чаще всего такие угрозы реализуются с использованием отчуждаемых носителей информации.

2. 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 программой общего пользования (например, системы управления базами данных), так и специально созданными для выполнения несанкционированного доступа программами. например:

- программами просмотра и модификации реестра;
- программами поиска текстов в текстовых файлах по ключевым словам 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.

3. 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.

4.2.4. Общая характеристика УБПДн, реализуемых с использованием протоколов межсетевого взаимодействия.

Классификация угроз, реализуемых по сети, приведена в Таблице 2. В ее основу положено семь первичных признаков классификации.

Таблица 2

№ п/п	Признак классификации	Тип угрозы	Описание
1	Характер угрозы	Пассивная угроза	угроза, при реализации которой не оказывается непосредственное влияние на работу ИСПДн, но могут быть нарушены установленные правила разграничения доступа к ПДн или сетевым ресурсам.
		Активная угроза	угроза, связанная с воздействием на ресурсы ИСПДн, при реализации которой оказывается непосредственное влияние на работу системы (изменение конфигурации, нарушение работоспособности и т.д.), с нарушением установленных правил разграничения доступа к ПДн или сетевым ресурсам.
2	Цель реализации угрозы	угрозы направленные на нарушение конфиденциальности	
		угрозы направленные на нарушение целостности	
		угрозы направленные на нарушение доступности	

3	Условие начала осуществления процесса реализации угрозы	по запросу от объекта, относительно которого реализуется угроза	нарушитель ожидает передачи запроса определенного типа, который и будет условием начала осуществления несанкционированного доступа
		по наступлению ожидаемого события на объекте, относительно которого реализуется угроза	нарушитель осуществляет постоянное наблюдение за состоянием операционной системы ИСПДн и при возникновении определенного события в этой системе начинает действовать несанкционированный доступ
		безусловное воздействие	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	с обратной связью	Между нарушителем и ИСПДн существует обратная связь, которая позволяет нарушителю адекватно реагировать на все изменения, происходящие в ИСПДн
		без обратной связи	Реализация угроз не требуется реагировать на какие-либо изменения, происходящие в ИСПДн
5	Расположение нарушителя относительно ИСПДн	внутрисегментно	подключение осуществляется к аппаратным элементам ИСПДн
		межсегментно	нарушитель может располагаться как вне ИСПДн, реализуя угрозу из другой сети, так в одном из сегментов ИСПДн, реализуя угрозу относительно технического средства ИСПДн, расположенного в другом сегменте ИСПДн
6	Уровень эталонной модели взаимодействия	Физический уровень модели ISO/OSI	
		Канальный уровень модели ISO/OSI	
		Сетевой уровень модели ISO/OSI	
		Транспортный уровень модели ISO/OSI	
		Сеансовый уровень модели ISO/OSI	
		Представительный уровень модели ISO/OSI	
		Прикладной уровень модели ISO/OSI	
7	Соотношение количества	угроза «один к одному»	Реализуется одним нарушителем относительно одного технического средства ИСПДн
		угроза «один ко многим»	Реализуется одним нарушителем относительно нескольких технических средств ИСПДн

	нарушителей и элементов ИСПДн, относительно которых реализуется угроза	распределенные или комбинированные угрозы	Реализуется несколькими нарушителями с разных компьютеров относительно одного или нескольких технических средств ИСПДн

С учетом проведенной классификации можно выделить **восемь** угроз, реализуемых с использованием протоколов межсетевого взаимодействия:

1. анализ сетевого трафика;
2. сканирование сети;
3. угроза выявления пароля;
4. подмена доверенного объекта сети и передача по каналам связи сообщений от его имени с присвоением его прав доступа;
5. навязывание ложного маршрута сети;
6. внедрение ложного объекта сети;
7. отказ в обслуживании;
8. удаленный запуск приложений.

4.2.4.1. 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 ИСПДн – 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;

– перехватывает 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 предусматривающих шифрование), ее подмены, модификации и т.п.

4.2.4.2. 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.

4.2.4.3. 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 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.

4.2.4.4. Подмена доверенного объекта сети и передача по каналам связи сообщений от его имени с присвоением его прав доступа

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 к техническому средству ИСПДн – цели угроз, установленные его пользователем для доверенного абонента.

4.2.4.5. 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.

4.2.4.6. 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. 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.

4.2.4.7. 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:

1. скрытый отказ в обслуживании, вызванный привлечением части ресурсов ИСПДн на обработку пакетов, передаваемых злоумышленником со снижением пропускной способности каналов связи, производительности сетевых устройств, нарушением требований к времени обработки запросов. Примерами реализации угроз подобного рода могут служить: направленный шторм эхо-запросов по протоколу ICMP (Ping flooding), шторм запросов на установление TCP-соединений (SYN-flooding), шторм запросов к FTP-серверу;

2. 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);**

3. явный отказ в обслуживании, вызванный нарушением логической связности между техническим средствами ИСПДн при передаче нарушителем управля-

ющих сообщений от имени сетевых устройств, приводящих к изменению маршрутно-адресных данных (например, ICMP Redirect Host, DNS-flooding) или идентификационной и аутентификационной информации;

4. 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 полная остановка ИСПДн из-за невозможности системы заниматься ничем другим, кроме обработки запросов.

4.2.4.8. 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.

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

2. Удаленный запуск приложения путем переполнения буфера приложений-серверов.

При угрозах этого подкласса используются недостатки программ, реализующих сетевые сервисы (в частности, отсутствие контроля за переполнением буфера). Настройкой системных регистров иногда удается переключить процессор после прерывания, вызванного переполнением буфера, на исполнение кода, содержащегося за границей буфера. Примером реализации такой угрозы может служить внедрение широко известного «вируса Морриса».

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

При угрозах этого подкласса нарушитель использует возможности удаленного управления системой, предоставляемые скрытыми компонентами (например, «троянскими» программами типа 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.

4.2.5. 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 (копирования, уничтожения, блокирования и т.п.);
- сохранять фрагменты информации из оперативной памяти в некоторых областях внешней памяти прямого доступа (локальных или удаленных);
- искажать произвольным образом, блокировать и (или) подменять выводимый во внешнюю память или в канал связи массив информации, образовавшийся в результате работы прикладных программ, или уже находящиеся во внешней памяти массивы данных.

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

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

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

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.

4.2.6. 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:

1. компьютерной стеганографии;
2. основанные на манипуляции различных характеристик ИСПДн, которые можно получать санкционированно (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.

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 форматов представления изображений. В настоящее время существует целый ряд доступных программных продуктов, реализующих известные стеганографические методы сокрытия информации. При этом преимущественно используются графические и аудио-контейнеры.

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.

4.2.7. Общая характеристика результатов несанкционированного или случайного доступа.

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

1. Нарушению конфиденциальности (копирование, неправомерное распространение), которое может быть осуществлено в случае утечки информации за счет:

- 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.

2. Нарушению целостности (уничтожение, изменение) 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.

3. Нарушению доступности (блокирование) 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.

4.3. Определение уровня исходной защищенности ИСПДн «Управление персоналом государственных органов»

Под уровнем исходной защищенности понимается обобщенный показатель, зависящий от технических и эксплуатационных характеристик ИСПДн (Y_1).

Таблица 3

Показатели исходной защищенности ИСПДн «Управление персоналом государственных органов»

Технические и эксплуатационные характеристики ИСПДн «Управление персоналом государственных органов»	Уровень защищенности		
	Высокий	Средний	Низкий
1. По территориальному размещению: локальная ИСПДн, развернутая в пределах одного здания.	+	–	-
2. По наличию соединения с сетями общего пользования: ИСПДн, физически отделенная от сети общего пользования	+	–	–
3. По встроенным (легальным) операциям с записями баз персональных данных: – чтение, поиск, запись, удаление, сортировка, модификация, передача.	-	+	–
4. По разграничению доступа к персональным данным: ИСПДн, к которой имеет доступ определенный перечень сотрудников организации, являющийся владельцем ИСПДн, либо субъект ПДн	–	+	–

5. По наличию соединений с другими базами ПДн иных ИСПДн: ИСПДн, в которой используется одна база ПДн, принадлежащая организации – владельцу данной ИСПДн	+	–	–
6. По уровню обобщения (обезличивания) ПДн: ИСПДн, в которой предоставляемые пользователю данные не являются обезличенными (т.е. присутствует информация, позволяющая идентифицировать субъекта ПДн)	-	–	+
7. По объему ПДн, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки: ИСПДн, не предоставляющие никакой информации	+	–	–

В соответствии с Таблицей 3, менее 70% характеристик ИСПДн соответствуют уровню не ниже "средний", следовательно Y_1=5.

ИСПДн имеет ***средний уровень*** исходной защищенности.

4.4. Определение вероятности реализации угроз в ИСПДн «Управление персоналом государственных органов»

Под вероятностью реализации угрозы поднимается определяемый экспертным путем показатель, характеризующий, насколько вероятным является реализации конкретной угрозы безопасности ПДн для данной ИСПДн в складывающихся условиях обстановки.

Вероятность (Y_2) определяется по 4 вербальным градациям этого показателя:

Таблица 4

Градация	Описание	Вероятность (Y2)
маловероятно	отсутствуют объективные предпосылки для осуществления угрозы	$Y_2 = 0$
низкая вероятность	объективные предпосылки для реализации угрозы существуют, но принятые меры существенно затрудняют ее реализацию	$Y_2 = 2$
средняя вероятность	объектные предпосылки для реализации угрозы существуют, но принятые меры обеспечения безопасности ПДн недостаточны	$Y_2 = 5$
высокая вероятность	объективные предпосылки для реализации угрозы существуют и меры по обеспечению безопасности ПДн не приняты	$Y_2 = 10$

Оценка вероятности реализации угрозы безопасности различными категориями нарушителей приведена в Таблице 5.

Таблица 5

Угроза безопасности ПДн	Вероятность реализации угрозы нарушителем категории Кn								
	$К_1$	$К_2$	$К_3$	$К_4$	$К_5$	$К_6$	$К_7$	$К_8$	Итог Y_2
угроза модификации базовой системы ввода/вывода (BIOS),	2	0	0	2	2	2	2	2	2
угроза перехвата управления загрузкой	0	0	0	0	2	2	2	0	0
угроза НСД с применением стандартных функций операционной системы	0	0	2	2	5	5	2	2	2
угроза НСД с помощью прикладной программы	0	0	2	2	2	2	2	0	2
угроза НСД с применением специально созданных для этого программ	0	0	2	0	0	0	2	0	0
угроза утечки информации с использованием копирования ее на съемные носители;	0	2	0	2	2	2	2	2	2
угроза утечки информации за счет ее несанкционированной передачи по каналам связи	0	2	2	2	2	2	2	0	2
угроза внедрения вредоносных программ с использованием съемных носителей	2	2	2	2	2	2	2	2	2
угроза «Анализа сетевого трафика»	2	0	0	2	2	2	0	0	2
угроза сканирования направленного на выявление открытых портов и служб, открытых соединений и др	2	0	0	2	2	2	0	0	2
угроза обхода системы идентификации и аутентификации сообщений	0	0	0	0	0	0	2	0	0
угроза обхода системы идентификации и аутентификации сетевых объектов	0	2	2	2	2	2	2	0	2
угроза внедрения ложного объекта сети	2	2	2	2	2	2	0	0	2
угроза навязывания ложного маршрута	2	2	2	2	2	2	0	0	2
угроза перехвата и взлома паролей	0	0	2	2	2	2	2	0	2
угроза подбора паролей доступа	2	2	2	2	2	2	2	0	2
угроза типа «Отказ в обслуживании»	2	0	0	2	2	2	0	0	2
угроза внедрения троянских программ	2	0	0	2	2	2	0	0	2

угроза атаки типа «переполнение буфера»;	2	0	0	2	2	2	2	0	2
угроза удаленного запуска приложений с использованием средств удаленного управления	0	0	0	2	2	2	2	0	2
угроза внедрения вредоносных программ через почтовые сообщения	2	0	0	2	2	2	0	0	2
угроза внедрения вредоносных программ через обмен и загрузку файлов	2	0	0	2	2	2	0	0	2
угроза заражения сетевыми червями, использующими уязвимости сетевого ПО	2	0	0	2	2	2	0	0	2

По итогам оценки уровня исходной защищенности (Y_1) и вероятности реализации угрозы (Y_2), рассчитывается коэффициент реализуемости угрозы (Y) и определяется возможность реализации угрозы (Таблица 6). Коэффициент реализуемости угрозы рассчитывается по формуле: $Y=(Y_1+Y_2)/20$.

Таблица 6

Угроза безопасности ПДн	**Коэффициент реализуемости угрозы (Y)**	**Возможность реализации угрозы**
угроза модификации базовой системы ввода/вывода (BIOS),	0,35	средняя
угроза перехвата управления загрузкой	0,25	низкая
угроза НСД с применением стандартных функций операционной системы	0,35	средняя
угроза НСД с помощью прикладной программы	0,35	средняя
угроза НСД с применением специально созданных для этого программ	0,25	низкая
угроза утечки информации с использованием копирования ее на съемные носители;	0,25	низкая
угроза утечки информации за счет ее несанкционированной передачи по каналам связи	0,35	средняя
угроза внедрения вредоносных программ с использованием съемных носителей	0,35	средняя
угроза «Анализа сетевого трафика»	0,35	средняя
угроза сканирования направленного на выявление открытых портов и служб, открытых соединений и др	0,35	средняя
угроза обхода системы идентификации и аутенти-	0,25	низкая

фикации сообщений		
угроза обхода системы идентификации и аутентификации сетевых объектов	0,35	средняя
угроза внедрения ложного объекта сети	0,35	средняя
угроза навязывания ложного маршрута	0,35	средняя
угроза перехвата и взлома паролей	0,35	средняя
угроза подбора паролей доступа	0,35	средняя
угроза типа «Отказ в обслуживании»	0,35	средняя
угроза внедрения троянских программ	0,35	средняя
угроза атаки типа «переполнение буфера»;	0,35	средняя
угроза удаленного запуска приложений с использованием средств удаленного управления	0,35	средняя
угроза внедрения вредоносных программ через почтовые сообщения	0,35	средняя
угроза внедрения вредоносных программ через обмен и загрузку файлов	0,35	средняя
угроза заражения сетевыми червями, использующими уязвимости сетевого ПО	0,35	средняя

4.5. Оценка опасности угроз ИСПДн **«Управление персоналом государственных органов».**

Оценка опасности определяется вербальным показателем опасности, который имеет 3 значения:

1. низкая опасность – если реализация угрозы может привести к незначительным негативным последствиям для субъектов персональных данных;

2. средняя опасность – если реализация угрозы может привести к негативным последствиям для субъектов персональных данных;

3. высокая опасность – если реализация угрозы может привести к значительным негативным последствиям для субъектов персональных данных.

Оценка опасности приведена в Таблице 7.

Таблица 7

Угроза безопасности ПДн	Опасность угроз
угроза модификации базовой системы ввода/вывода (BIOS),	низкая
угроза перехвата управления загрузкой	низкая
угроза НСД с применением стандартных функций операционной системы	низкая
угроза НСД с помощью прикладной программы	низкая
угроза НСД с применением специально созданных для этого программ	низкая
угроза утечки информации с использованием копирования ее на съемные носители;	низкая
угроза утечки информации за счет ее несанкционированной передачи по каналам связи	низкая
угроза внедрения вредоносных программ с использованием съемных носителей	низкая
угроза «Анализа сетевого трафика»	низкая

угроза сканирования направленного на выявление открытых портов и служб, открытых соединений и др.	низкая
угроза обхода системы идентификации и аутентификации сообщений	низкая
угроза обхода системы идентификации и аутентификации сетевых объектов	низкая
угроза внедрения ложного объекта сети	низкая
угроза навязывания ложного маршрута	низкая
угроза перехвата и взлома паролей	низкая
угроза подбора паролей доступа	низкая
угроза типа «Отказ в обслуживании»	низкая
угроза внедрения троянских программ	низкая
угроза атаки типа «переполнение буфера»	низкая
угроза удаленного запуска приложений с использованием средств удаленного управления	низкая
угроза внедрения вредоносных программ через почтовые сообщения	низкая
угроза внедрения вредоносных программ через обмен и загрузку файлов	низкая
угроза заражения сетевыми червями, использующими уязвимости сетевого ПО	низкая

5. Перечень актуальных УБПДн в ИСПДн «Управление персоналом государственных органов».

Отнесение угрозы к актуальной производится по правилам, приведенным в Таблице 8.

Таблица 8

Возможность реализации угрозы	Показатель опасности угрозы		
	Низкая	Средняя	Высокая
Низкая	неактуальная	неактуальная	актуальная
Средняя	неактуальная	актуальная	актуальная
Высокая	актуальная	актуальная	актуальная
Очень высокая	актуальная	актуальная	актуальная

В соответствии с правилами отнесения угроз безопасности к актуальным, для ИСПДн «Управление персоналом государственных органов» существуют следующие актуальные угрозы (Таблица 9).

Таблица 9

Угроза безопасности ПДн	Опасность угроз
угроза модификации базовой системы ввода/вывода (BIOS)	неактуальная
угроза перехвата управления загрузкой	неактуальная

угроза НСД с применением стандартных функций операционной системы	неактуальная
угроза НСД с помощью прикладной программы	неактуальная
угроза НСД с применением специально созданных для этого программ	неактуальная
угроза утечки информации с использованием копирования ее на съемные носители	неактуальная
угроза утечки информации за счет ее несанкционированной передачи по каналам связи	неактуальная
угроза внедрения вредоносных программ с использованием съемных носителей	неактуальная
угроза «Анализа сетевого трафика»	неактуальная
угроза сканирования направленного на выявление открытых портов и служб, открытых соединений и др.	неактуальная
угроза обхода системы идентификации и аутентификации сообщений	неактуальная
угроза обхода системы идентификации и аутентификации сетевых объектов	неактуальная
угроза внедрения ложного объекта сети	неактуальная
угроза навязывания ложного маршрута	неактуальная
угроза перехвата и взлома паролей	неактуальная
угроза подбора паролей доступа	неактуальная
угроза типа «Отказ в обслуживании»	неактуальная
угроза внедрения троянских программ	неактуальная
угроза атаки типа «переполнение буфера»;	неактуальная
угроза удаленного запуска приложений с использованием средств удаленного управления	неактуальная
угроза внедрения вредоносных программ через почтовые сообщения	неактуальная
угроза внедрения вредоносных программ через обмен и загрузку файлов	неактуальная
угроза заражения сетевыми червями, использующими уязвимости сетевого ПО	неактуальная

Таким образом, актуальных угроз безопасности ПДн в ИСПДн «Управление персоналом государственных органов» не выявлено.

Заключение

В настоящем документе проведена классификация УБПДн в ИСПДн «Управление персоналом государственных органов» дано общее описание УБПДн и построена Модель угроз.

Построенная Модель угроз безопасности ПДн в ИСПДн «Управление персоналом государственных органов» применима к существующему состоянию ИСПДн «Управление персоналом государственных органов» при условии соблюдения основных (базовых) исходных данных:

- технические средства ИСПДн находятся в пределах контролируемой зоны;
- ИСПДн физически отделена от сетей общего пользования;
- отсутствует возможность неконтролируемого пребывания посторонних лиц в служебных помещениях ИСПДн и др.

В случае несоблюдения и/или изменения вышеуказанных условий Модель угроз безопасности ПДн в ИСПДн «Управление персоналом государственных органов» должна быть пересмотрена.