



УТВЕРЖДАЮ

Руководитель Юго-Восточного
управления МОиН СО
Е.Ю.Баландина
Приказ от 14.10.2019 № 434-од

Модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных Юго-Восточного управления министерства образования и науки Самарской области

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, характеризующееся способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных.

Биометрические персональные данные - сведения, которые характеризуют физиологические особенности человека и на основе которых можно установить его личность, включая фотографии, отпечатки пальцев, образ сетчатки глаза, особенности строения тела и другую подобную информацию.

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 (ИСПДн) - 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.

Использование персональных данных - действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц.

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

Контролируемая зона - пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также 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.

Неавтоматизированная обработка персональных данных - обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы, считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.

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, 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.

Обезличивание персональных данных - действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных.

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.

Общедоступные персональные данные - персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

Оператор (персональных данных) - 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 - 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, применяемые в информационных системах.

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.

Политика "чистого стола" - комплекс организационных мероприятий, контролирующих отсутствие записывания на бумажные носители ключей и атрибутов доступа (паролей) и хранения их вблизи объектов доступа.

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, заблокировать, уничтожить информацию или уничтожить и модифицировать программное обеспечение информационной системы персональных данных и (или) заблокировать аппаратные средства.

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

Раскрытие персональных данных - умышленное или случайное нарушение конфиденциальности персональных данных.

Распространение персональных данных - действия, направленные на передачу персональных данных определенному кругу лиц (передача

персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом.

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

Специальные категории персональных данных - персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья и интимной жизни субъекта персональных данных.

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.

Трансграничная передача персональных данных - передача персональных данных оператором через Государственную границу Российской Федерации органу власти иностранного государства, физическому или юридическому лицу иностранного государства.

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.

Учреждение - государственное бюджетное учреждение дополнительного профессионального образования Самарской области «Нефтегорский Ресурсный центр».

Уязвимость - слабость в средствах защиты, 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).

Обозначения и сокращения

АВС - антивирусные средства

АРМ - автоматизированное рабочее место

ВТСС - вспомогательные технические средства и системы

ИСПДн - информационная система персональных данных

КЗ - контролируемая зона

ЛВС - локальная вычислительная сеть

МЭ - межсетевой экран

НСД - несанкционированный доступ

ОС - операционная система

ПДн - персональные данные

ПМВ - программно-математическое воздействие

ПО - программное обеспечение

ПЭМИН - побочные электромагнитные излучения и наводки

САЗ - система анализа защищенности

СЗИ - средства защиты информации

СЗПДн - система (подсистема) защиты персональных данных

СОВ - система обнаружения вторжений

ТКУ И - технические каналы утечки информации

УБПДн - угрозы безопасности персональных данных

Введение

Модель угроз безопасности персональных данных (далее - Модель) при их обработке в ИСПДн

- 1) РИС «Планирование ГИА-9».
- 2) РИС «Планирование ГИА-11».
- 3) БД Кадры.
- 4) АИС «1С: Бухгалтерия и заработная плата».
- 5) АИС Контур –экстерн.
- 6) АИС «УРМ – Бюджет».
- 7) АИС «ПФР».
- 8) АИС «Налогоплательщик».
- 9) ФИС ФРДО

строится на основании Отчета о результатах проведения внутренней проверки.

В модели угроз представлено описание структуры ИСПДн, состава и режима обработки ПДн, классификацию потенциальных нарушителей, оценку исходного уровня защищенности, анализ угроз безопасности персональных данных.

Анализ УБПДн включает:

- Описание угроз.
- Оценку вероятности возникновения угроз.
- Оценку реализуемости угроз.
- Оценку опасности угроз.
- Определение актуальности угроз.

В заключении даны рекомендации по мерам защиты для уменьшения опасности актуальных угроз.

| | | | |
|--------------------------------|---|---|--------------------|
| Операторы ИСПДн правами записи | Обладает всеми необходимыми атрибутами и правами, обеспечивающими доступ ко всем ПДн. | - сбор - систематизация - накопление - хранение - уточнение - использование - уничтожение | Отдел регистратуры |
|--------------------------------|---|---|--------------------|

Для обработки ПДн используется ПО, указанное в таблице 2.

Таблица 2 – ПО, используемое для обработки ПДн

| Наименование | Назначение |
|---|--|
| Microsoft Windows 7 Professional Service Pack 1 | Операционная система |
| Kaspersky Endpoint Security | Антивирус |
| 7-Zip 16.02 | Архиватор |
| Adobe Reader XI – Russian | ПО для просмотра файлов в формате PDF Google Chrome Браузер |
| Microsoft Office профессиональный плюс 2007 | Пакет офисных приложений |

1.1. Классификация нарушителей

По признаку принадлежности к ИСПДн все нарушители делятся на две группы:

- внешние нарушители - физические лица, не имеющие права пребывания на территории контролируемой зоны, в пределах которой размещается оборудование ИСПДн;
- внутренние нарушители - физические лица, имеющие право пребывания на территории контролируемой зоны, в пределах которой размещается оборудование ИСПДн.

1.1.1. Внешний нарушитель

В качестве внешнего нарушителя информационной безопасности, рассматривается нарушитель, который не имеет непосредственного доступа к техническим средствам и ресурсам системы, находящимся в пределах контролируемой зоны.

Предполагается, что внешний нарушитель не может воздействовать на защищаемую информацию по техническим каналам утечки, так как объем информации, хранимой и обрабатываемой в ИСПДн, является недостаточным для возможной мотивации внешнего нарушителя к осуществлению действий, направленных на утечку информации по техническим каналам утечки.

Предполагается, что внешний нарушитель может воздействовать на защищаемую информацию только во время ее передачи по каналам связи.

1.1.2. Внутренний нарушитель

Возможности внутреннего нарушителя существенным образом зависят от действующих в пределах контролируемой зоны ограничительных факторов, из которых основным является реализация комплекса организационно-технических мер, в том числе по подбору, расстановке и обеспечению высокой профессиональной подготовки кадров, допуску физических лиц внутрь контролируемой зоны и контролю за порядком проведения работ, направленных на предотвращение и пресечение несанкционированного доступа.

Система разграничения доступа ИСПДн обеспечивает разграничение прав пользователей на доступ к информационным, программным, аппаратным и другим ресурсам ИСПДн в соответствии с принятой политикой информационной безопасности (правилами). К внутренним нарушителям могут относиться:

- администраторы ИСПДн (категория I);
- администраторы конкретных подсистем или баз данных ИСПДн (категория II);
- пользователи ИСПДн (категория III);
- пользователи, являющиеся внешними по отношению к конкретной АС (категория IV);

- лица, обладающие возможностью доступа к системе передачи данных (категория V);
- сотрудники ЛПУ, имеющие санкционированный доступ в служебных целях в помещения, в которых размещаются элементы ИСПДн, но не имеющие права доступа к ним (категория VI);
- обслуживающий персонал ЛПУ (охрана, работники инженерно-технических служб и т.д.) (категория VII);
- уполномоченный персонал разработчиков ИСПДн, который на договорной основе имеет право на техническое обслуживание и модификацию компонентов ИСПДн (категория VIII).

На лиц категорий I и II возложены задачи по администрированию программно-аппаратных средств и баз данных ИСПДн для интеграции и обеспечения взаимодействия различных подсистем, входящих в состав ИСПДн. Администраторы потенциально могут реализовывать угрозы ИБ, используя возможности по непосредственному доступу к защищаемой информации, обрабатываемой и хранимой в ИСПДн, а также к техническим и программным средствам ИСПДн, включая средства защиты, используемые в конкретных АС, в соответствии с установленными для них административными полномочиями.

Эти лица хорошо знакомы с основными алгоритмами, протоколами, реализуемыми и используемыми в конкретных подсистемах и ИСПДн в целом, а также с применяемыми принципами и концепциями безопасности.

Предполагается, что они могли бы использовать стандартное оборудование либо для идентификации уязвимостей, либо для реализации угроз ИБ. Данное оборудование может быть как частью штатных средств, так и может относиться к легко получаемому (например, программное обеспечение, полученное из общедоступных внешних источников).

Кроме того, предполагается, что эти лица могли бы располагать специализированным оборудованием.

К лицам категорий I и II ввиду их исключительной роли в ИСПДн должен применяться комплекс особых организационно-режимных мер по их подбору, принятию на работу, назначению на должность и контролю выполнения функциональных обязанностей.

Предполагается, что в число лиц категорий I и II будут включаться только доверенные лица и поэтому указанные лица исключаются из числа вероятных нарушителей.

Предполагается, что лица категорий III-VIII относятся к вероятным нарушителям.

Предполагается, что возможность сговора внутренних нарушителей маловероятна ввиду принятых организационных и контролирующих мер.

1.1.3. Предположения об имеющейся у нарушителя информации об объектах реализации угроз

В качестве основных уровней знаний нарушителей об АС можно выделить следующие:

- общая информация - информации о назначения и общих характеристиках ИСПДн;
- эксплуатационная информация - информация, полученная из эксплуатационной документации;
- чувствительная информация - информация, дополняющая эксплуатационную информацию об ИСПДн (например, сведения из проектной документации ИСПДн).

В частности, нарушитель может иметь:

- данные об организации работы, структуре и используемых технических, программных и программно-технических средствах ИСПДн;
- сведения об информационных ресурсах ИСПДн: порядок и правила создания, хранения и передачи информации, структура и свойства информационных потоков;
- данные об уязвимостях, включая данные о недокументированных (недекларированных) возможностях технических, программных и программно-технических средств ИСПДн;
- данные о реализованных в ПСЗИ принципах и алгоритмах;
- исходные тексты программного обеспечения ИСПДн;
- сведения о возможных каналах реализации угроз;
- информацию о способах реализации угроз.

Предполагается, что лица категории III и категории IV владеют только эксплуатационной информацией, что обеспечивается организационными мерами. При этом лица категории IV не владеют парольной,

аутентифицирующей и ключевой информацией, используемой в АИС, к которым они не имеют санкционированного доступа.

Предполагается, что лица категории V владеют в той или иной части чувствительной и эксплуатационной информацией о системе передачи информации и общей информацией об АИС, использующих эту систему передачи информации, что обеспечивается организационными мерами. При этом лица категории V не владеют парольной и аутентифицирующей информацией, используемой в АИС.

Предполагается, что лица категории VI и лица категории VII по уровню знаний не превосходят лица категории V.

Предполагается, что лица категории VIII обладают чувствительной информацией об ИСПДн и функционально ориентированных АИС, включая информацию об уязвимостях технических и программных средств ИСПДн. Организационными мерами предполагается исключить доступ лиц категории VIII к техническим и программным средствам ИСПДн в момент обработки с использованием этих средств защищаемой информации.

Таким образом, наиболее информированными об АИС являются лица категории III и лица категории VIII.

Степень информированности нарушителя зависит от многих факторов, включая реализованные в ЛПУ конкретные организационные меры и компетенцию нарушителей. Поэтому объективно оценить объем знаний вероятного нарушителя в общем случае практически невозможно.

В связи с изложенным, с целью создания определенного запаса прочности предполагается, что вероятные нарушители обладают всей информацией, необходимой для подготовки и реализации угроз, за исключением информации, доступ к которой со стороны нарушителя исключается системой защиты информации. К такой информации, например, относится парольная, аутентифицирующая и ключевая информация.

1.6.4 Предположения об имеющихся у нарушителя средствах реализации угроз

Предполагается, что нарушитель имеет:

- аппаратные компоненты СЗПДн и СФ СЗПДн;
- доступные в свободной продаже технические средства и программное обеспечение;

- специально разработанные технические средства и программное обеспечение.

Внутренний нарушитель может использовать штатные средства.

Состав имеющихся у нарушителя средств, которые он может использовать для реализации угроз ИБ, а также возможности по их применению зависят от многих факторов, включая реализованные на объектах ЛПУ конкретные организационные меры, финансовые возможности и компетенцию нарушителей. Поэтому объективно оценить состав имеющихся у нарушителя средств реализации угроз в общем случае практически невозможно.

Поэтому, для создания устойчивой СЗПДн предполагается, что вероятный нарушитель имеет все необходимые для реализации угроз средства, возможности которых не превосходят возможности аналогичных средств реализации угроз на информацию, содержащую сведения, составляющие государственную тайну, и технические и программные средства, обрабатывающие эту информацию.

Вместе с тем предполагается, что нарушитель не имеет:

- средств перехвата в технических каналах утечки;
- средств воздействия через сигнальные цепи (информационные и управляющие интерфейсы СВТ);
- средств воздействия на источники и через цепи питания;
- средств воздействия через цепи заземления;
- средств активного воздействия на технические средства (средств облучения).

Предполагается, что наиболее совершенными средствами реализации угроз обладают лица категории III и лица категории VIII.

| | Низкая | Средняя | Высокая |
|---------------|--------------|--------------|------------|
| Низкая | неактуальная | неактуальная | актуальная |
| Средняя | неактуальная | актуальная | актуальная |
| Высокая | актуальная | актуальная | актуальная |
| Очень высокая | актуальная | актуальная | актуальная |

Оценка актуальности угроз безопасности представлена в таблице.

Таблица 7 - Актуальность УБПДн

| Тип угроз безопасности ПДн | Опасность угрозы |
|--|------------------|
| 1. Угрозы от утечки по техническим каналам. | |
| 1.1. Угрозы утечки акустической информации | Низкая |
| 1.2. Угрозы утечки видовой информации | Низкая |
| 1.3. Угрозы утечки информации по каналам ПЭМИН | Низкая |
| 2. Угрозы несанкционированного доступа к информации. | |
| 2.1. Угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИСПДн | |
| 2.1.1. Кража ПЭВМ | Низкая |
| 2.1.2. Кража носителей информации | Средняя |
| 2.1.3. Кража ключей и атрибутов доступа | Средняя |
| 2.1.4. Кражи, модификации, уничтожения информации | Низкая |
| 2.1.5. Вывод из строя узлов ПЭВМ, каналов связи | Низкая |
| 2.1.6. Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ | Низкая |
| 2.1.7. Несанкционированное отключение средств защиты | Низкая |
| 2.2. Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий). | |
| 2.2.1. Действия вредоносных программ (вирусов) | Средняя |
| 2.2.2. Недекларированные возможности системного ПО и ПО для обработки персональных данных | Низкая |
| 2.2.3. Установка ПО не связанного с исполнением служебных обязанностей | Средняя |
| 2.3. Угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПДн в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера. | |
| 2.3.1. Утрата ключей и атрибутов доступа | Средняя |
| 2.3.2. Непреднамеренная модификация (уничтожение) информации сотрудниками | Средняя |
| 2.3.3. Непреднамеренное отключение средств защиты | Низкая |
| 2.3.4. Выход из строя аппаратно-программных средств | Средняя |
| 2.3.5. Сбой системы электроснабжения | Средняя |
| 2.3.6. Стихийное бедствие | Низкая |
| 2.4. Угрозы преднамеренных действий внутренних нарушителей | |
| 2.4.1. Доступ к информации, модификация, уничтожение лиц не | Низкая |

| | |
|--|--------|
| допущенных к ее обработке | |
| 2.4.2. Разглашение информации, модификация, уничтожение сотрудниками допущенными к ее обработке | Низкая |
| 2.5. Угрозы несанкционированного доступа по каналам связи. | |
| 2.5.1. Угроза "Анализ сетевого трафика" с перехватом передаваемой из ИСПДн и принимаемой из внешних сетей информации: | Низкая |
| 2.5.1.1. Перехват за пределами контролируемой зоны | Низкая |
| 2.5.1.2. Перехват в пределах контролируемой зоны внешними нарушителями | Низкая |
| 2.5.1.3. Перехват в пределах контролируемой зоны внутренними нарушителями. | Низкая |
| 2.5.2. 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. | Низкая |
| 2.5.3. Угрозы выявления паролей по сети | Низкая |
| 2.5.4. Угрозы навязывание ложного маршрута сети | Низкая |
| 2.5.5. Угрозы подмены доверенного объекта в сети | Низкая |
| 2.5.6. Угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях | Низкая |
| 2.5.7. Угрозы типа "Отказ в обслуживании" | Низкая |
| 2.5.8. Угрозы удаленного запуска приложений | Низкая |
| 2.5.9. Угрозы внедрения по сети вредоносных программ | Низкая |

Были выявлены следующие актуальные угрозы:

- 1) Кража носителей информации.
- 2) Кража ключей и атрибутов доступа.
- 3) Действия вредоносных программ (вирусов).
- 4) Установка ПО не связанного с исполнением служебных обязанностей.
- 5) Утрата ключей и атрибутов доступа.
- 6) Непреднамеренная модификация (уничтожение) информации сотрудниками.
- 7) Выход из строя аппаратно-программных средств.
- 8) Сбой системы электроснабжения.

Для снижения опасности реализации актуальных УБПДн рекомендуется осуществить следующие мероприятия:

- 1) Контроль над соблюдением режима обработки ПДн - Ежедневно.
- 2) Контроль над соблюдением режима защиты – Ежедневно.

- 3) Контроль над выполнением антивирусной защиты – Ежедневно.
- 4) Организация анализа и пересмотра имеющихся угроз безопасности ПДн, а так же предсказание появления новых, еще неизвестных, угроз - Ежегодно.
- 5) Поддержание в актуальном состоянии нормативно-организационных документов –Ежемесячно.

Заключение

В соответствии Постановление Правительства РФ от 1 ноября 2012 г. N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных для персональных данных ИСПДн) РИС «Планирование ГИА-9», РИС «Планирование ГИА-11», БД Кадры, АИС «1С: Бухгалтерия и заработная плата», АИС Контур –экстерн, АИС «УРМ – Бюджет», АИС «ПФР», АИС «Налогоплательщик», необходимо обеспечивать 4 Уровень защищенности персональных данных при их обработке в информационной системе.,

Аттестация ИСПДн РИС «Планирование ГИА-9» не требуется.

Аттестация ИСПДн РИС «Планирование ГИА-11» не требуется.

Аттестация ИСПДн БД Кадры не требуется.

Аттестация ИСПДн АИС «1С: Бухгалтерия и заработная плата» не требуется.

Аттестация ИСПДн АИС Контур –экстерн не требуется.

Аттестация ИСПДн АИС «УРМ – Бюджет» не требуется.

Аттестация ИСПДн АИС «ПФР» не требуется.

Аттестация ИСПДн АИС «Налогоплательщик» не требуется.

Аттестация ФИС ФРДО- аттестат соответствия информационной системы персональных данных «Автоматизированное рабочее место оператора ФИС ФРДО» требованиям безопасности информации - №105/2019-АТ от 17.07.2019г.