**РОССИЙСКАЯ ФЕДЕРАЦИЯ**

**АДМИНИСТРАЦИЯ ТРУБЧЕВСКОГО МУНИЦИПАЛЬНОГО РАЙОНА**

**Р А С П О Р Я Ж Е Н И Е**

от 23.10.2015г. № 807-р

г. Трубчевск

|  |
| --- |
| Об утверждении частной модели угроз безопасности  персональных данных при их обработке в информационной  системе персональных данных администрации Трубчевского муниципального района «СБиС++» |

Во исполнение требований Федерального закона от 27.07.2006 № 152 «О персональных данных», постановления Правительства Российской Федерации от 01.11.2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Приказа ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», в соответствии с Методикой определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденной ФСТЭК России 14.02.2008, а также иных нормативных документов по защите информации:

  1. Утвердить прилагаемую частную модель угроз безопасности персональных данных при их обработке в информационной системе персональных данных администрации Трубчевского муниципального района «СБиС++».

 2. Контроль за исполнением настоящего распоряжения возложить на заместителя главы администрации Трубчевского муниципального района Тубол С.Н.

**Глава администрации**

**Трубчевского муниципального района И.И. Обыдённов**

Утверждена

распоряжением администрации

Трубчевского муниципального района

от 23.10. 2015г. № 807-р

Частная модель угроз безопасности персональных данных при их обработке в информационной системе персональных данных администрации Трубчевского муниципального района «СБиС++»

Термины и Определения

Автоматизированная система – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая [информационную технологию](http://pandia.ru/text/category/informatcionnie_tehnologii/) выполнения установленных функций.

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](http://pandia.ru/text/category/virus/) 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.

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](http://pandia.ru/text/category/informatcionnie_seti/)).

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 – электрический сигнал, 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](http://pandia.ru/text/category/bazi_dannih/), 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 соответствующими 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 и 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.

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 и 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 записи ключей и атрибутов доступа (паролей) на бумажные носители 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, блокировать, уничтожить информацию или уничтожить и модифицировать [программное обеспечение](http://pandia.ru/text/category/programmnoe_obespechenie/) информационной системы персональных данных и / или блокировать 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](http://pandia.ru/text/category/sredstva_massovoj_informatcii/), 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 и 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.

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.

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 – Администрация Трубчевского муниципального района.

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](http://pandia.ru/text/category/avtomatizirovannie_sistemi/) обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

Обозначения и сокращения

|  |  |  |
| --- | --- | --- |
| АВС | - | антивирусные средства |
| АИС | - | автоматизированная информационная система |
| АРМ | - | автоматизированное рабочее место |
| ИНН | - | индивидуальный номер налогоплательщика |
| ИСПДн | - | информационная система персональных данных |
| ЛВС | - | локальная вычислительная сеть |
| ЛИС | - | локальная информационная система |
| МЭ | - | межсетевой экран |
| НСД | - | несанкционированный доступ |
| ОС | - | операционная система |
| ПДн | - | персональные данные |
| ПМВ | - | программно-математическое воздействие |
| ПО | - | программное обеспечение |
| ПФ | - | [пенсионный фонд](http://pandia.ru/text/category/pensionnij_fond/) |
| ПЭМИН | - | побочные электромагнитные излучения и наводки |
| РИС | - | распределенная информационная система |
| СЗИ | - | средства защиты информации |
| СЗПДн | - | система (подсистема) защиты персональных данных |
| ТКУИ | - | технические каналы утечки информации |
| УБПДн | - | угрозы безопасности персональных данных |
| ФСТЭК России | - | Федеральная служба по техническому и экспортному контролю – федеральный орган исполнительной власти России, осуществляющим реализацию государственной политики, организацию межведомственной координации и взаимодействия, специальные и контрольные функции в области государственной безопасности. |

Введение

Обработка персональных данных в Администрации Трубчевского муниципального района осуществляется в информационной системе персональных данных (далее – ИСПДн) «СБиС++».

Модель угроз безопасности персональных данных (далее – Модель) при их обработке в ИСПДн «СБиС++» строится на основании Отчета о результатах проведения внутренней проверки.

В Модели угроз представлено описание структуры ИСПДн, состава и режима обработки ПДн, классификации 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.

1 ИСПДн «СБиС++»

Структура ИСПДн

Таблица 1. Параметры ИСПДн

|  |  |
| --- | --- |
| Заданные характеристики безопасности персональных данных | Специальная информационная система |
| Структура информационной системы | Автоматизированное рабочее место |
| Подключение информационной системы к сетям общего пользования и (или) сетям международного информационного обмена | Подключена |
| Режим обработки персональных данных | Однопользовательская |
| Режим разграничения прав доступа пользователей | Система с разграничением прав доступа |
| Местонахождение технических средств информационной системы | Все технические средства находятся в пределах Российской Федерации |
| Дополнительные информация | К персональным данным предъявляется требование целостности и (или) доступности |

Состав и структура персональных данных

В ИСПДн обрабатываются следующие персональные данные:

- фамилия, имя, отчество сотрудников

- паспортные данные сотрудников

- сведения о месте регистрации

- СНИЛС

- ИНН.

Исходя из состава обрабатываемых персональных данных, можно сделать вывод, что они относятся ко 2 категории персональных данных, т. е. к данным, позволяющим идентифицировать субъекта персональных данных и получить о нем дополнительную информацию, за исключением персональных данных, относящихся к категории 1.

Объем обрабатываемых персональных данных, не превышает 1000 записей о субъектах персональных данных.

Структура обработки ПДн

В ИСПДн «СБиС++» обработка персональных данных происходит следующим образом:

- сотрудник авторизуется на своем рабочем месте в ОС [Microsoft](http://pandia.ru/text/category/microsoft/) Windows 7.0;

- сотрудник авторизуется в «СБиС++»;

- cотрудник вносит персональные данные о сотрудниках;

- данные отправляются в соответствующие органы и удаляются с АРМ.

Режим обработки ПДн

В ИСПДн «СБиС++» обработка персональных данных осуществляется в однопользовательском режиме с разграничением прав доступа.

Режим обработки предусматривает следующие действия с персональными данными: сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, уничтожение персональных данных.

Все пользователи ИСПДн имеют собственные роли. Список типовых ролей представлен в таблице.

Таблица 2. Матрица доступа

|  |  |  |
| --- | --- | --- |
| Группа | Уровень доступа к ПДн | Разрешенные действия |
| Администраторы ИСПДн | Обладает полной информацией о системном и прикладном программном обеспечении ИСПДн.  Обладает полной информацией о технических средствах и конфигурации ИСПДн.  Имеет доступ ко всем техническим средствам обработки информации и данным ИСПДн.  Обладает правами конфигурирования и административной настройки технических средств ИСПДн | сбор  систематизация  накопление  хранение  уточнение  использование  уничтожение |
| Администратор безопасности | Обладает правами Администратора ИСПДн.  Обладает полной информацией об ИСПДн.  Имеет доступ к средствам защиты информации и протоколирования и к части ключевых элементов ИСПДн.  Не имеет прав доступа к конфигурированию технических средств сети за исключением контрольных (инспекционных) | сбор  систематизация  накопление  хранение  уточнение  использование  уничтожение |
| Операторы ИСПДн с правами записи | Обладает всеми необходимыми атрибутами и правами, обеспечивающими доступ ко всем ПДн | сбор  систематизация  накопление  хранение  уточнение  использование  уничтожение |
| Операторы ИСПДн с правами чтения | Обладает всеми необходимыми атрибутами и правами, обеспечивающими доступ к подмножеству ПДн | использование |

Классификация нарушителей

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

- внешние нарушители – физические лица, осуществляющие целенаправленное деструктивное воздействие, 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](http://pandia.ru/text/category/informatcionnaya_bezopasnostmz/) 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 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

К такому виду нарушителя могут относиться (список лиц должен быть уточнен в соответствии с группами пользователей описанных в Политике информационной безопасности):

- пользователи ИСПДн, т. е. сотрудники, имеющие право доступа к ИСПДн (категория I);

- сотрудники, не имеющие права доступа к ИСПДн (категория II);

- администраторы ИСПДн (категория III);

- разработчики и поставщики программно-технических средств, расходных материалов, услуг (категория IV).

Возможности нарушителей 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.

Лица категорий I и III 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 данных категорий 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.

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;

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 I владеют только эксплуатационной информацией, что обеспечивается организационными мерами.

Предполагается, что лица категории III обладают чувствительной информацией об ИСПДн и функционально ориентированных АИС, включая информацию об уязвимостях технических и программных средств ИСПДн.

Степень информированности нарушителя зависит от многих факторов, включая реализованные 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.

1.1.4 Предположения об имеющихся у нарушителя средствах реализации угроз

Предполагается, что нарушитель имеет:

- аппаратные компоненты СЗПДн;

- доступные в свободной продаже технические средства и [программное обеспечение](http://pandia.ru/text/category/programmnoe_obespechenie/);

- специально разработанные технические средства и программное обеспечение.

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 IV.

Необходимо определить всех потенциальных нарушителей, не имеющих доступа в ИСПДн, всех пользователей ИСПДн и определить их категорию.

Исходный уровень защищенности ИСПДн

Под общим уровнем защищенности понимается обобщенный показатель, зависящий от технических и эксплуатационных характеристик ИСПДн (Y1).

В таблице представлены характеристики уровня исходной защищенности для ИСПДн «СБиС++».

Таблица 3. Исходный уровень защищенности

|  |  |  |
| --- | --- | --- |
| Позиция | Технические и эксплуатационные характеристики | Уровень  защищенности |
| 1 | По территориальному размещению | высокий |
| 2 | По наличию соединения с сетями общего пользования | средний |
| 3 | По встроенным (легальным) операциям с записями баз персональных данных | средний |
| 4 | По разграничению доступа к персональным данным | средний |
| 5 | По наличию соединений с другими базами ПДн иных ИСПДн | средний |
| 6 | По уровню (обезличивания) ПДн | высокий |
| 7 | По объему ПДн, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки | средний |

Вероятность реализации УБПДн

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

Числовой коэффициент (Y2) для оценки вероятности возникновения угрозы определяется по 4 вербальным градациям этого показателя:

- маловероятно - отсутствуют объективные предпосылки для осуществления угрозы (Y2 = 0);

- низкая вероятность - объективные предпосылки для реализации угрозы существуют, но принятые меры существенно затрудняют ее реализацию (Y2 = 2);

- средняя вероятность *-* объективные предпосылки для реализации угрозы существуют, но принятые меры обеспечения безопасности ПДн недостаточны (Y2 = 5);

- высокая вероятность *-* объективные предпосылки для реализации угрозы существуют и меры по обеспечению безопасности ПДн не приняты (Y2 = 10).

При обработке персональных данных в ИСПДн можно выделить следующие угрозы.

1.1.5 Угрозы утечки информации по техническим каналам

1.1.5.1 Угрозы утечки акустической (речевой) информации

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

В ИСПДн Учреждений функции голосового ввода ПДн или функции воспроизведения ПДн акустическими средствами отсутствуют. Поэтому для всех видов ИСПДн вероятность реализации угрозы – является маловероятной.

1.1.5.2 Угрозы утечки видовой информации

Реализация угрозы утечки видовой информации возможна за счет просмотра информации с помощью оптических (оптико-электронных) 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.

Если в Учреждении введен контроль доступа в контролируемую зону, АРМ пользователей расположены так, что практически исключен визуальный доступ к мониторам, а на окнах установлены жалюзи, то для всех типов ИСПДн вероятность реализации угрозы – является маловероятной.

Если в Учреждении отсутствуют вышеперечисленные меры защиты, то их необходимо внедрить.

1.1.5.3 Угрозы утечки информации по каналам ПЭМИН

Угрозы утечки информации по каналу ПЭМИН, возможны из-за наличия паразитных электромагнитных излучений у элементов ИСПДн.

Угрозы данного класса маловероятны для всех видов ИСПДн, т. к. размер контролируемой зоны большой, и элементы ИСПДн зачастую находятся в самом центре здания и экранируются несколькими несущими стенами, а паразитный сигнал маскируется со множеством других паразитных сигналов элементов, не входящих в ИСПДн.

1.1.6 Угрозы несанкционированного доступа к информации путем физического доступа к элементам ИСПДн, носителям персональных данных, ключам и атрибутам доступа

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

- нарушению конфиденциальности (копирование, неправомерное распространение);

- нарушению целостности (уничтожение, изменение);

- нарушению доступности (блокирование).

1.1.6.1 Кража и уничтожение носителей информации

Угроза осуществляется всеми видами нарушителей.

Если в Учреждении введен контроль доступа в контролируемую зону, установлена охранная сигнализация, двери закрываются на замок, установлены решетки на первых и последних этажах здания, ведется учет и хранение носителей в сейфе, то для всех видов ИСПДн вероятность реализации угрозы – является маловероятной.

При наличии свободного доступа в контролируемую зону посторонних лиц вероятность реализации угрозы должна быть пересмотрена, и необходимо принять меры по пресечению НСД посторонних лиц к носителям информации.

1.1.6.2 Кража физических носителей ключей и атрибутов доступа

Угроза осуществляется всеми видами нарушителей.

Вероятность реализации угрозы повышается при наличии свободного доступа в контролируемую зону посторонних лиц.

Если в Учреждении введен контроль доступа в контролируемую зону, установлена охранная сигнализация, двери закрываются на замок, установлены решетки на первых и последних этажах здания, ведется учет и хранение носителей в сейфе, то для всех видов ИСПДн вероятность реализации угрозы – является низкой.

При отсутствии парольной политики или контроля за ее исполнением, вероятность реализации угрозы должна быть пересмотрена, и необходимо принять меры по организации парольной политики.

1.1.6.3 Утрата носителей информации

Угроза осуществляется внутренними нарушителями, являющимися пользователями ИСПДн, вследствие человеческого фактора.

Если в Учреждении осуществляется учет носителей информации и пользователи проинструктированы о действиях в случаях утраты носителей, то для всех видов ИСПДн вероятность реализации угрозы – является маловероятной.

1.1.6.4 Утрата и компрометация ключей и атрибутов доступа

Угроза осуществляется за счет действия человеческого фактора пользователей ИСПДн, которые нарушают положения парольной политики в части их создания (создают простые или пустые пароли, не меняют пароли по истечении срока их жизни или компрометации и т. п.) и хранения (записывают пароли на бумажные носители, передают ключи доступа третьим лицам и т. п.) или не осведомлены о них.

Если в Учреждении введена парольная политика, предусматривающая требуемую сложность пароля и периодическую его смену, введена политика «чистого стола», осуществляется контроль за выполнением правил политик, пользователи проинструктированы о парольной политике и о действиях в случаях утраты или компрометации паролей, то для всех видов ИСПДн вероятность реализации угрозы – является низкой.

При отсутствии парольной политики или контроля за ее исполнением, вероятность реализации угрозы должна быть пересмотрена, и необходимо принять меры по организации парольной политики.

1.1.7 Угрозы несанкционированного доступа к информации с использованием программно-аппаратных и программных средств

1.1.7.1 Доступ к информации, ее модификация и уничтожение лицами, не имеющими прав доступа

Угроза осуществляется внешними нарушителями и внутренними нарушителями категорий II и IV там, где расположены элементы ИСПДн и средства защиты, а так же происходит работа пользователей.

Если в Учреждении введен контроль доступа в контролируемую зону, установлена охранная сигнализация, двери закрываются на замок, установлены решетки на первых и последних этажах здания, то для всех видов ИСПДн вероятность реализации угрозы – является маловероятной.

При наличии свободного доступа в контролируемую зону посторонних лиц, вероятность реализации угрозы должна быть пересмотрена, и необходимо принять меры по пресечению НСД в контролируемую зону.

1.1.7.2 Утечка информации через порты ввода/вывода

Угроза осуществляется внутренними нарушителями категорий I и IV.

Угроза реализуется путем подключения съемных носителей к компьютеру и несанкционированного копирования на них информации.

Если в Учреждении порты ввода/вывода изолированы, пользователи ознакомлены с политикой безопасности, то для всех видов ИСПДн вероятность реализации угрозы – является низкой.

Вероятность реализации угрозы может быть пересмотрена при отсутствии ограничений использования съемных носителей информации.

1.1.7.3 Воздействие вредоносных программ ([вирусов](http://pandia.ru/text/category/virus/))

Программно-математическое воздействие - это воздействие с помощью вредоносных программ. Программой с потенциально опасными последствиями или вредоносной программой (вирусом) 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.

Если в Учреждении на всех элементах ИСПДн установлена антивирусная защита, пользователи проинструктированы о мерах предотвращения вирусного заражения, то для всех видов ИСПДн вероятность реализации угрозы – является низкой.

При отсутствии установленной антивирусной защиты, вероятность реализации угрозы должна быть пересмотрена, и необходимо принять меры по предотвращению угроз вирусного заражения.

1.1.7.4 Установка ПО, не связанного с исполнением служебных обязанностей

Угроза осуществляется путем несанкционированной установки ПО внутренними нарушителями категорий I и IV.

Если в Учреждении введено разграничение прав пользователей на установку ПО и осуществляется контроль, пользователи проинструктированы о политике установки ПО, то для всех видов ИСПДн вероятность реализации угрозы – является низкой.

При отсутствии разграничения прав на установку ПО, вероятность реализации угрозы должна быть пересмотрена, и необходимо принять меры по организации разграничения прав пользователей.

1.1.7.5 Внедрение или сокрытие недекларированных возможностей системного ПО и ПО для обработки персональных данных

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

Если в Учреждении осуществляется контроль действий пользователей и разработчиков, то для всех видов ИСПДн вероятность реализации угрозы – является маловероятной.

При увеличении элементов, в том числе программного обеспечения, ИСПДн, числа функциональных связей между элементами и при наличии подключения к сетям общего доступа и (или) международного обмена вероятность реализации данной угрозы должна быть пересмотрена.

Для снижения вероятности реализации угрозы необходимо сертифицировать ПО собственной разработки или стандартное ПО, доработанное под нужды учреждения.

1.1.7.6 Создание учетных записей теневых пользователей и неучтенных точек доступа в систему

Угроза осуществляется внутренними нарушителями категорий I и IV.

Угроза реализуется путем несанкционированного создания неучтенных точек доступа в систему (например, несанкционированное подключение нового компьютера к локальной сети), а также создание нерабочих учетных записей (тестовых, временных и т. д.).

Вероятность реализации угрозы повышается при отсутствии контроля действий пользователей и разработчиков.

Вероятность реализации угрозы – является маловероятной.

1.1.8 Угрозы несанкционированного доступа к информации по каналам связи

1.1.8.1 Угроза «Анализ сетевого трафика» с перехватом информации за пределами контролируемой зоны

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.

Вероятность реализации угрозы для всех видов ИСПДн – является маловероятной.

1.1.8.2 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.

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.

Вероятность реализации угрозы для всех видов ИСПДн – является маловероятной.

1.1.8.3 Угроза выявления паролей по сети

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.

Вероятность реализации угрозы – является низкой.

1.1.8.4 Угрозы типа «Отказ в обслуживании»

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

Могут быть выделены несколько разновидностей таких угроз:

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

- 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);

- явный отказ в обслуживании, вызванный нарушением логической связности между техническим средствами ИСПДн при передаче нарушителем управляющих сообщений от имени сетевых устройств, приводящих к изменению маршрутно-адресных данных (например, ICMP Redirect Host, DNS-flooding) или идентификационной и аутентификационной информации;

- явный отказ в обслуживании, вызванный передачей злоумышленником пакетов с нестандартными атрибутами (угрозы типа «Land», «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, которое 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.

Если в Учреждении обрабатываемые ПДн не пересылаются по сетям общего пользования и международного обмена, то вероятность реализации угрозы – является маловероятной.

Во всех других случаях должна быть оценена вероятность реализации угрозы.

1.1.8.5 Угрозы внедрения по сети вредоносных программ

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

Вредоносными программами, обеспечивающими осуществление НСД, могут быть:

- программы подбора и вскрытия паролей;

- программы, реализующие угрозы;

- программы, демонстрирующие использование недекларированных возможностей программного и программно-аппаратного обеспечения ИСПДн;

- программы-генераторы компьютерных вирусов;

- программы, демонстрирующие уязвимости средств защиты информации и др.

Если в Учреждении обрабатываемые ПДн не пересылаются по сетям общего пользования и международного обмена, установлена антивирусная защита, то вероятность реализации угрозы – является маловероятной.

Во всех других случаях должна быть оценена вероятность реализации угрозы.

1.1.8.6 Утечка информации, передаваемой с использованием протоколов беспроводного доступа

Угроза реализуется путем перехвата информации, передаваемой по беспроводным сетям.

Если в Учреждении производится контроль трафика, проходящего по беспроводным сетям, то вероятность реализации угрозы – является маловероятной.

Во всех других случаях должна быть оценена вероятность реализации угрозы.

1.1.8.7 Перехват, модификация закрытого ключа ЭЦП

Угроза реализуется путем получения доступа к закрытому ключу ЭЦП либо путем перехвата закрытого ключа ЭЦП.

Вероятность реализации угрозы – является маловероятной.

1.1.8.8 Угрозы удаленного запуска 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:

- распространение файлов, содержащих несанкционированный исполняемый код;

- удаленный запуск приложения путем переполнения [буфера](http://pandia.ru/text/category/bufer/) приложений-серверов;

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

Типовые угрозы первого из указанных подклассов основываются на активизации распространяемых файлов при случайном обращении к ним. Примерами таких файлов могут служить: файлы, содержащие исполняемый код в вид документы, содержащие исполняемый код в виде элементов ActiveX, Java-апплетов, интерпретируемых скриптов (например, тексты на JavaScript); файлы, содержащие исполняемые коды программ. Для распространения файлов могут использоваться службы электронной почты, передачи файлов, сетевой файловой системы.

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

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

Если в Учреждении обрабатываемые ПДн не пересылаются по сетям общего пользования и международного обмена, установлена антивирусная защита, то вероятность реализации угрозы – является маловероятной.

Во всех других случаях должна быть оценена вероятность реализации угрозы.

1.1.9 Угрозы антропогенного характера

1.1.9.1 Разглашение информации

Угроза осуществляется внутренними нарушителями категорий I и III.

Угроза реализуется путем несанкционированной передачи информации третьим лицам.

Если в Учреждении пользователи осведомлены о порядке работы с персональными данными, а также подписали Договор о неразглашении, то для всех видов ИСПДн вероятность реализации угрозы – является низкой.

При неосведомленности пользователей и не заключении Договора о неразглашении, вероятность реализации угрозы должна быть пересмотрена, и необходимо принять меры снижению вероятности реализации угрозы.

1.1.9.2 Сокрытие ошибок и неправомерных действий пользователей и администраторов

Угроза реализуется внутренними нарушителями категорий I и III.

Если в Учреждении осуществляется контроль действий пользователей, то для всех видов ИСПДн вероятность реализации угрозы – является маловероятной.

При отсутствии контроля действий пользователей вероятность реализации угрозы должна быть пересмотрена, и необходимо принять меры по установлению контроля.

1.1.9.3 Угроза появления новых уязвимостей вследствие невыполнения ответственными лицами своих должностных обязанностей

Угроза реализуется внутренними нарушителями категории III.

Угроза реализуется вследствие халатного отношения ответственного лица к своим должностным обязанностям.

Если в Учреждении осуществляется контроль действий ответственных лиц, то для всех видов ИСПДн вероятность реализации угрозы – является маловероятной.

При отсутствии контроля действий ответственных лиц вероятность реализации угрозы должна быть пересмотрена, и необходимо принять меры по установлению контроля.

1.1.9.4 Угроза нарушения политики предоставления и прекращения доступа

Угроза реализуется внутренними нарушителями категории III.

Угроза реализуется при отсутствии процедуры удаления устаревших, неучтенных или недействующих учетных записей пользователей или несанкционированного предоставления прав доступа.

Вероятность реализации угрозы повышается при отсутствии контроля действий администраторов.

Вероятность реализации угрозы – является маловероятной.

1.1.9.5 Непреднамеренная модификация (уничтожение) информации

Угроза реализуется внутренними нарушителями категорий I и III.

Угроза реализуется путем непреднамеренного воздействия на элементы ИСПДн или содержащуюся в ней информацию.

Если в Учреждении осуществляется резервное копирование обрабатываемых ПДн, пользователи проинструктированы о работе с ИСПДн, то для всех видов ИСПДн вероятность реализации угрозы – является маловероятной.

При отсутствии резервного копирования и неосведомленности пользователей о работе с ИСПДн, вероятность реализации угрозы должна быть пересмотрена, и необходимо принять меры снижению вероятности реализации угрозы.

1.1.9.6 Непреднамеренное отключение средств защиты

Угроза реализуется внутренними нарушителями категорий I и III.

Угроза реализуется путем случайного отключения средств защиты (антивирусного ПО, межсетевых экранов и т. д.).

Вероятность реализации угрозы повышается при отсутствии контроля доступа в контролируемую зону и к настройкам режимов средств защиты, а так же неосведомленности пользователей о работе с ИСПДн.

Вероятность реализации угрозы для всех видов ИСПДн – является маловероятной.

1.1.10 Угрозы воздействия непреодолимых сил

1.1.10.1 Стихийное бедствие

Угроза осуществляется вследствие возникновения различного рода природных катаклизмов (землетрясение, затопление и прочее).

Если в Учреждении сотрудники проинструктированы о действиях в случае возникновения внештатных ситуаций, то для всех видов ИСПДн вероятность реализации угрозы – является маловероятной.

При отсутствии пожарной сигнализации и неосведомленности пользователей о действиях в случае возникновения внештатных ситуаций, вероятность реализации угрозы должна быть пересмотрена, и необходимо принять меры снижению вероятности реализации угрозы.

1.1.10.2 Выход из строя аппаратно-программных средств

Угроза реализуется вследствие окончания срока эксплуатации аппаратно-программных средств, нерегулярных проверок данных средств и перебоев в электропитании.

Если в Учреждении производится своевременная замена устаревших аппаратно-программных средств, регулярные проверки аппаратно-программных средств и установлены элементы бесперебойного питания, то для всех видов ИСПДн вероятность реализации угрозы – является маловероятной.

В противном случае вероятность реализации угрозы должна быть пересмотрена, и необходимо принять меры снижению вероятности реализации угрозы.

1.1.10.3 Аварии (пожар, потоп, случайное отключение электричества)

Угроза осуществляется вследствие возникновения различного рода аварий в пределах контролируемой зоны.

Если в Учреждении производится своевременная замена устаревшего оборудования, коммуникаций и т. д., проводятся их регулярные проверки, установлены элементы бесперебойного питания, то для всех видов ИСПДн вероятность реализации угрозы – является маловероятной.

В противном случае вероятность реализации угрозы должна быть пересмотрена, и необходимо принять меры снижению вероятности реализации угрозы.

Реализуемость угроз

По итогам оценки уровня защищенности (Y1) и вероятности реализации угрозы (Y2), рассчитывается коэффициент реализуемости угрозы (Y) и определяется возможность реализации угрозы. Коэффициент реализуемости угрозы Y будет определяться соотношением Y = (Y1 + Y2)/20.

Оценка реализуемости УБПДн представлена в таблице.

Таблица 4. Реализуемость УБПДн

|  |  |  |
| --- | --- | --- |
| Тип угроз безопасности ПДн | Коэффициент реализуемости угрозы (Y) | Возможность реализации |
| 1. Угрозы от утечки по техническим каналам |  |  |
| 1.1. Угрозы утечки акустической информации | 0,25 | низкая |
| 1.2. Угрозы утечки видовой информации | 0,25 | низкая |
| 1.3. Угрозы утечки информации по каналам ПЭМИН | 0,25 | низкая |
| 2. Угрозы несанкционированного доступа к информации путем физического доступа к элементам ИСПДн, носителям персональных данных, ключам и атрибутам доступа |  |  |
| 2.1. Кража и уничтожение носителей информации | 0,25 | низкая |
| 2.2. Кража физических носителей ключей и атрибутов доступа | 0,25 | средняя |
| 2.3. Утрата носителей информации | 0,25 | низкая |
| 2.4. Утрата и компрометация ключей и атрибутов доступа | 0,35 | средняя |
| 3. Угрозы несанкционированного доступа к информации с использованием программно-аппаратных и программных средств |  |  |
| 3.1. Доступ к информации, ее модификация и уничтожение лицами, не имеющими прав доступа | 0,35 | низкая |
| 3.2. Утечка информации через порты ввода/вывода | 0,25 | средняя |
| 3.3. Воздействие вредоносных программ ([вирусов](http://pandia.ru/text/category/virus/)) | 0,35 | средняя |
| 3.4. Установка ПО, не связанного с исполнением служебных обязанностей | 0,35 | средняя |
| 3.5. Внедрение или сокрытие недекларированных возможностей системного ПО и ПО для обработки персональных данных | 0,35 | низкая |
| 3.6. Создание учетных записей теневых пользователей и неучтенных точек доступа в систему | 0,25 | низкая |
| 4. Угрозы несанкционированного доступа к информации по каналам связи |  |  |
| 4.1. Угроза «Анализ сетевого трафика» с перехватом информации за пределами контролируемой зоны | 0,25 | низкая |
| 4.2. 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. | 0,25 | низкая |
| 4.3. Угрозы выявления паролей по сети | 0,25 | средняя |
| 4.4. Угрозы типа «Отказ в обслуживании» | 0,25 | низкая |
| 4.5. Угрозы внедрения по сети вредоносных программ | 0,25 | низкая |
| 4.6.Утечка информации, передаваемой с использованием протоколов беспроводного доступа | 0,25 | низкая |
| 4.7. Перехват, модификация закрытого ключа ЭЦП | 0,25 | низкая |
| 4.8. Угрозы удаленного запуска приложений | 0,25 | низкая |
| 5. Угрозы антропогенного характера |  |  |
| 5.1. Разглашение информации | 0,35 | средняя |
| 5.2. Сокрытие ошибок и неправомерных действий пользователей и администраторов | 0,35 | низкая |
| 5.3. Угроза появления новых уязвимостей вследствие невыполнения ответственными лицами своих должностных обязанностей | 0,25 | низкая |
| 5.4. Угроза нарушения политики предоставления и прекращения доступа | 0,25 | низкая |
| 5.5. Непреднамеренная модификация (уничтожение) информации | 0,35 | низкая |
| 5.6. Непреднамеренное отключение средств защиты | 0,25 | низкая |
| 6. Угрозы воздействия непреодолимых сил |  |  |
| 6.1. Стихийное бедствие | 0,25 | низкая |
| 6.2. Выход из строя аппаратно-программных средств | 0,25 | низкая |
| 6.3. Аварии (пожар, потоп, случайное отключение электричества) | 0,25 | низкая |

Оценка опасности угроз

Оценка опасности УБПДн производится на основе опроса специалистов по защите информации и определяется вербальным показателем опасности, который имеет три значения:

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

- средняя опасность - если реализация угрозы может привести к негативным последствиям для субъектов персональных данных;

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

Оценка опасности УБПДн представлена в таблице.

Таблица 5. Опасность 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 путем физического доступа к элементам ИСПДн, носителям персональных данных, ключам и атрибутам доступа |  |
| 2.1. Кража и уничтожение носителей информации | низкая |
| 2.2. Кража физических носителей ключей и атрибутов доступа | средняя |
| 2.3. Утрата носителей информации | низкая |
| 2.4. Утрата и компрометация ключей и атрибутов доступа | средняя |
| 3. Угрозы несанкционированного доступа к информации с использованием программно-аппаратных и программных средств |  |
| 3.1. Доступ к информации, ее модификация и уничтожение лицами, не имеющими прав доступа | низкая |
| 3.2. Утечка информации через порты ввода/вывода | средняя |
| 3.3. Воздействие вредоносных программ (вирусов) | средняя |
| 3.4. Установка ПО, не связанного с исполнением служебных обязанностей | средняя |
| 3.5. Внедрение или сокрытие недекларированных возможностей системного ПО и ПО для обработки персональных данных | низкая |
| 3.6. Создание учетных записей теневых пользователей и неучтенных точек доступа в систему | низкая |
| 4. Угрозы несанкционированного доступа к информации по каналам связи |  |
| 4.1. Угроза «Анализ сетевого трафика» с перехватом информации за пределами контролируемой зоны | низкая |
| 4.2. 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 |
| 4.3. Угрозы выявления паролей по сети | низкая |
| 4.4. Угрозы типа «Отказ в обслуживании» | низкая |
| 4.5. Угрозы внедрения по сети вредоносных программ | низкая |
| 4.6.Утечка информации, передаваемой с использованием протоколов беспроводного доступа | низкая |
| 4.7. Перехват, модификация закрытого ключа ЭЦП | низкая |
| 4.8. Угрозы удаленного запуска приложений | низкая |
| 5. Угрозы антропогенного характера |  |
| 5.1. Разглашение информации | средняя |
| 5.2. Сокрытие ошибок и неправомерных действий пользователей и администраторов | низкая |
| 5.3. Угроза появления новых уязвимостей вследствие невыполнения ответственными лицами своих должностных обязанностей | низкая |
| 5.4. Угроза нарушения политики предоставления и прекращения доступа | низкая |
| 5.5. Непреднамеренная модификация (уничтожение) информации | низкая |
| 5.6. Непреднамеренное отключение средств защиты | низкая |
| 6. Угрозы воздействия непреодолимых сил |  |
| 6.1. Стихийное бедствие | низкая |
| 6.2. Выход из строя аппаратно-программных средств | низкая |
| 6.3. Аварии (пожар, потоп, случайное отключение электричества) | низкая |

Определение актуальности угроз в ИСПДн

В соответствии с правилами отнесения угрозы безопасности к актуальной, для ИСПДн определяются актуальные и неактуальные угрозы.

Таблица 6. Правила определения актуальности УБПДн

|  |  |
| --- | --- |
| 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 |

Оценка актуальности угроз безопасности представлена в таблице.

Таблица 7. Актуальность УБПДн

|  |  |
| --- | --- |
| Тип угроз безопасности ПДн | Актуальность  угрозы |
| 1. Угрозы от утечки по техническим каналам. |  |
| 1.1. Угрозы утечки акустической информации | неактуальная |
| 1.2. Угрозы утечки видовой информации | неактуальная |
| 1.3. Угрозы утечки информации по каналам ПЭМИН | неактуальная |
| 2. Угрозы несанкционированного доступа к информации путем физического доступа к элементам ИСПДн, носителям персональных данных, ключам и атрибутам доступа |  |
| 2.1. Кража и уничтожение носителей информации | неактуальная |
| 2.2. Кража физических носителей ключей и атрибутов доступа | актуальная |
| 2.3. Утрата носителей информации | неактуальная |
| 2.4. Утрата и компрометация ключей и атрибутов доступа | актуальная |
| 3. Угрозы несанкционированного доступа к информации с использованием программно-аппаратных и программных средств |  |
| 3.1. Доступ к информации, ее модификация и уничтожение лицами, не имеющими прав доступа | неактуальная |
| 3.2. Утечка информации через порты ввода/вывода | актуальная |
| 3.3. Воздействие вредоносных программ ([вирусов](http://pandia.ru/text/category/virus/)) | актуальная |
| 3.4. Установка ПО, не связанного с исполнением служебных обязанностей | актуальная |
| 3.5. Внедрение или сокрытие недекларированных возможностей системного ПО и ПО для обработки персональных данных | неактуальная |
| 3.6. Создание учетных записей теневых пользователей и неучтенных точек доступа в систему | неактуальная |
| 4. Угрозы несанкционированного доступа к информации по каналам связи |  |
| 4.1. Угроза «Анализ сетевого трафика» с перехватом информации за пределами контролируемой зоны | неактуальная |
| 4.2. 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. | неактуальная |
| 4.3. Угрозы выявления паролей по сети | актуальная |
| 4.4. Угрозы типа «Отказ в обслуживании» | неактуальная |
| 4.5. Угрозы внедрения по сети вредоносных программ | неактуальная |
| 4.6.Утечка информации, передаваемой с использованием протоколов беспроводного доступа | неактуальная |
| 4.7. Перехват, модификация закрытого ключа ЭЦП | неактуальная |
| 4.8. Угрозы удаленного запуска приложений | неактуальная |
| 5. Угрозы антропогенного характера |  |
| 5.1. Разглашение информации | актуальная |
| 5.2. Сокрытие ошибок и неправомерных действий пользователей и администраторов | неактуальная |
| 5.3. Угроза появления новых уязвимостей вследствие невыполнения ответственными лицами своих должностных обязанностей | неактуальная |
| 5.4. Угроза нарушения политики предоставления и прекращения доступа | неактуальная |
| 5.5. Непреднамеренная модификация (уничтожение) информации | неактуальная |
| 5.6. Непреднамеренное отключение средств защиты | неактуальная |
| 6. Угрозы воздействия непреодолимых сил |  |
| 6.1. Стихийное бедствие | неактуальная |
| 6.2. Выход из строя аппаратно-программных средств | неактуальная |
| 6.3. Аварии (пожар, потоп, случайное отключение электричества) | неактуальная |

Были выявлены следующие актуальные угрозы:

- кража физических носителей ключей и атрибутов доступа;

- утрата и компрометация ключей и атрибутов доступа;

- утечка информации через порты ввода/вывода;

- воздействие вредоносных программ (вирусов);

- установка ПО, не связанного с исполнением служебных обязанностей;

- угрозы выявления паролей по сети;

- разглашение информации.

Для снижения опасности реализации актуальных УБПДн рекомендуется осуществить следующие мероприятия:

- установка антивирусной защиты;

- парольная политика, устанавливающая обязательную сложность и периодичность смены пароля;

- назначить ответственного за безопасность персональных данных из числа сотрудников учреждения;

- инструкции пользователей ИСПДн, в которых отражены порядок безопасной работы с ИСПДн, а так же с ключами и атрибутами доступа;

- осуществление резервирования ключевых элементов ИСПДн;

- изолирование портов ввода/вывода;

- организация разграничения прав пользователей на установку стороннего ПО, установку аппаратных средств, подключения мобильных устройств и внешних носителей, установку и настройку элементов ИСПДн и средств защиты.

Модель угроз безопасности

Исходный класс защищенности – средний

Таблица 8. Угрозы безопасности

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Наименование угрозы | Вероятность реализации угрозы (Y2) | Возможность реализации угрозы (Y) | Опасность угрозы | Актуальность угрозы | Меры по противодействию угрозе |
| Технические | Организационные |  |  |  |  |
| 1. Угрозы от утечки по техническим каналам |  |  |  |  |  |
| 1.1. Угрозы утечки акустической информации | Маловероятно | Низкая | Низкая | Неактуальная | Виброгенераторы, генераторы шумов, звукоизоляция. | Инструкция пользователя |
| Технологический процесс |  |  |  |  |  |  |
| 1.2. Угрозы утечки видовой информации | Маловероятно | Низкая | Низкая | Неактуальная | Жалюзи на окна | Пропускной режим |
| Инструкция пользователя |  |  |  |  |  |  |
| 1.3. Угрозы утечки информации по каналам ПЭМИН | Маловероятно | Низкая | Низкая | Неактуальная | Генераторы пространственного зашумления | Технологический процесс обработки |
| Генератор шума по цепи электропитания | Контур заземления |  |  |  |  |  |
| 2. Угрозы несанкционированного доступа к информации путем физического доступа к элементам ИСПДн, носителям персональных данных, ключам и атрибутам доступа |  |  |  |  |  |  |
| 2.1. Кража и уничтожение носителей информации | Маловероятно | Низкая | Низкая | Неактуальная | Охранная сигнализация | Акт установки средств защиты |
| Хранение в сейфе | Учет носителей информации |  |  |  |  |  |
| Шифрование данных |  |  |  |  |  |  |
| 2.2. Кража физических носителей ключей и атрибутов доступа | Низкая | Средняя | Средняя | Актуальная | Хранение в сейфе | Инструкция пользователя |
|  |  |  |  |  |  |  |
| 2.3. Утрата носителей информации | Маловероятно | Низкая | Низкая | Неактуальная |  | Инструкция пользователя |
| Инструкция администратора безопасности |  |  |  |  |  |  |
| 2.4. Утрата и компрометация ключей и атрибутов доступа | Низкая | Средняя | Средняя | Актуальная |  | Инструкция пользователя |
| Инструкция администратора безопасности |  |  |  |  |  |  |
| 3. Угрозы несанкционированного доступа к информации с использованием программно-аппаратных и программных средств |  |  |  |  |  |  |
| 3.1. Доступ к информации, ее модификация и уничтожение лицами, не имеющими прав доступа | Маловероятно | Низкая | Низкая | Неактуальная | Система защиты от НСД | Акт установки средств защиты |
| Разрешительная система допуска |  |  |  |  |  |  |
| Технологический процесс обработки |  |  |  |  |  |  |
| 3.2. Утечка информации через порты ввода/вывода | Низкая | Средняя | Средняя | Актуальная | Изолирование портов ввода/вывода | Инструкция пользователя |
| 3.3. Воздействие вредоносных программ (вирусов) | Низкая | Средняя | Средняя | Актуальная | Антивирусное ПО | Инструкция пользователя |
| Инструкция ответственного |  |  |  |  |  |  |
| Инструкция администратора безопасности |  |  |  |  |  |  |
| Технологический процесс обработки |  |  |  |  |  |  |
| Инструкция по антивирусной защите |  |  |  |  |  |  |
| Акт установки средств защиты |  |  |  |  |  |  |
| 3.4. Установка ПО не связанного с исполнением служебных обязанностей | Низкая | Средняя | Средняя | Актуальная |  | Инструкция пользователя |
| Инструкция ответственного |  |  |  |  |  |  |
| 3.5. Внедрение или сокрытие недекларированных возможностей системного ПО и ПО для обработки персональных данных | Маловероятно | Низкая | Низкая | Неактуальная |  | Сертификация |
| 3.6. Создание учетных записей теневых пользователей и неучтенных точек доступа в систему | Маловероятно | Низкая | Низкая | Неактуальная | Система управления доступом | Инструкция пользователя |
| Инструкция ответственного |  |  |  |  |  |  |
| Инструкция администратора безопасности |  |  |  |  |  |  |
| 4. Угрозы несанкционированного доступа к информации по каналам связи |  |  |  |  |  |  |
| 4.1. Угроза «Анализ сетевого трафика» с перехватом информации за пределами контролируемой зоны | Маловероятно | Низкая | Низкая | Неактуальная | Межсетевой экран | Технологический процесс |
| Инструкция пользователя |  |  |  |  |  |  |
| Инструкция администратора безопасности |  |  |  |  |  |  |
| Акт установки средств защиты |  |  |  |  |  |  |
| 4.2. 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. | Маловероятно | Низкая | Низкая | Неактуальная | Межсетевой экран | Технологический процесс |
| Инструкция пользователя |  |  |  |  |  |  |
| Инструкция администратора безопасности |  |  |  |  |  |  |
| Акт установки средств защиты |  |  |  |  |  |  |
| 4.3. Угрозы выявления паролей по сети | Низкая | Средняя | Средняя | Актуальная | Межсетевой экран | Технологический процесс |
| Инструкция пользователя |  |  |  |  |  |  |
| Инструкция администратора безопасности |  |  |  |  |  |  |
| Акт установки средств защиты |  |  |  |  |  |  |
| 4.4. Угрозы типа «Отказ в обслуживании» | Маловероятно | Низкая | Низкая | Неактуальная | Межсетевой экран  Антивирусное ПО | Технологический процесс |
| Инструкция пользователя |  |  |  |  |  |  |
| Инструкция администратора безопасности |  |  |  |  |  |  |
| Резервирование |  |  |  |  |  |  |
| 4.5. Угрозы внедрения по сети вредоносных программ | Маловероятно | Низкая | Низкая | Неактуальная | Антивирусное ПО | Технологический процесс |
| Инструкция пользователя |  |  |  |  |  |  |
| Инструкция администратора безопасности |  |  |  |  |  |  |
| Акт установки средств защиты |  |  |  |  |  |  |
| 4.6. Утечка информации, передаваемой с использованием протоколов беспроводного доступа | Маловероятно | Низкая | Низкая | Неактуальная | Шифрование информации | Технологический процесс |
| Инструкция пользователя |  |  |  |  |  |  |
| Инструкция администратора безопасности |  |  |  |  |  |  |
| Акт установки средств защиты |  |  |  |  |  |  |
| 4.7. Перехват, модификация закрытого ключа ЭЦП | Маловероятно | Низкая | Низкая | Неактуальная | Межсетевой экран  Антивирусное ПО | Технологический процесс |
| Инструкция пользователя |  |  |  |  |  |  |
| Инструкция администратора безопасности |  |  |  |  |  |  |
| Акт установки средств защиты |  |  |  |  |  |  |
| 4.8. Угрозы удаленного запуска приложений | Маловероятно | Низкая | Низкая | Неактуальная | Межсетевой экран  Антивирусное ПО | Технологический процесс |
| Инструкция пользователя |  |  |  |  |  |  |
| Инструкция администратора безопасности |  |  |  |  |  |  |
| Акт установки средств защиты |  |  |  |  |  |  |
| 5. Угрозы антропогенного характера |  |  |  |  |  |  |
| 5.1. Разглашение информации | Низкая | Средняя | Средняя | Актуальная |  | Договор о неразглашении |
| Инструкция пользователя |  |  |  |  |  |  |
| 5.2. Сокрытие ошибок и неправомерных действий пользователей и администраторов | Маловероятно | Низкая | Низкая | Неактуальная |  | Договор о неразглашении |
| Инструкция пользователя |  |  |  |  |  |  |
| 5.3. Угроза появления новых уязвимостей вследствие невыполнения ответственными лицами своих должностных обязанностей | Маловероятно | Низкая | Низкая | Неактуальная |  | Договор о неразглашении |
| Инструкция пользователя |  |  |  |  |  |  |
| 5.4. Угроза нарушения политики предоставления и прекращения доступа | Маловероятно | Низкая | Низкая | Неактуальная |  | Договор о неразглашении |
| Инструкция пользователя |  |  |  |  |  |  |
| 5.5. Непреднамеренная модификация (уничтожение) информации | Маловероятно | Низкая | Низкая | Неактуальная | Настройка средств защиты | Резервное копирование |
| 5.6. Непреднамеренное отключение средств защиты | Маловероятно | Низкая | Низкая | Неактуальная | Доступ к установлению режимов работы средств защиты предоставляется только администратору безопасности | Инструкция пользователя |
| Инструкция администратора безопасности |  |  |  |  |  |  |
| 6. Угрозы воздействия непреодолимых сил |  |  |  |  |  |  |
| 6.1. Стихийное бедствие | Маловероятно | Низкая | Низкая | Неактуальная | Пожарная сигнализация | Инструкции по безопасности |
| 6.2. Выход из строя аппаратно-программных средств | Маловероятно | Низкая | Низкая | Неактуальная | Устройство бесперебойного питания | Резервирование |
| Инструкции по безопасности |  |  |  |  |  |  |
| 6.3. Аварии (пожар, потоп, случайное отключение электричества) | Маловероятно | Низкая | Низкая | Неактуальная | Пожарная сигнализация | Инструкции по безопасности |

2 Заключение

На основании категории и объема обрабатываемых персональных данных –

**ИСПДн «СБиС++» классифицируется как специальная ИСПДн класса K3.**

Аттестация ИСПДн «СБиС++» не требуется.