«УТВЕРЖДАЮ»

Директор ГКОУ «С(к)ш№10» г. Орска

_____ С.П. Онищенко

ЧАСТНАЯ МОДЕЛЬ УГРОЗ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ, ОБРАБАТЫВАЕМЫХ В СБИС++

Члены комиссии:

_____

_____

_____

_____

Орск,2023

Аннотация

Настоящий документ содержит описание модели угроз информационной безопасности персональных данных, обрабатываемых в ИСПДН СБИС++.

Модель угроз разработана в соответствии со следующими нормативными документами:

- Федеральным законом Российской Федерации от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральным законом Российской Федерации от 27 июля 2006 года № 152-ФЗ «О персональных данных»;
- Указом Президента Российской Федерации от 17 марта 2008 года № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена»;
- Указом Президента Российской Федерации от 5 декабря 2016 года № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации».
- Постановление Правительства Российской Федерации № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» от 01 ноября 2012 года;
- Приказом ФСТЭК России от 18 февраля 2013 года № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
- Приказом ФСБ России от 10 июля 2014 г. N 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»;
- РД Гостехкомиссии России «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации;
- РД Гостехкомиссии России «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации»;
- Положением о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005), утвержденным приказом ФСБ России от 9 февраля 2005 г. N 66, зарегистрировано Министерством юстиции Российской Федерации от 3 марта 2005 года № 6382.
- ГОСТ Р 51275-2006 «Защита информации. Факторы, воздействующие на информацию. Общие положения».

Настоящая модель угроз разработана на основании информации, полученной в результате обследования информационной системы персональных данных «СБИС++».

1. Введение

Настоящая модель угроз определяет перечень актуальных угроз безопасности персональным данным (далее - ПДн), обрабатываемых в ИСПДн СБИС++, и предназначена для:

определения уровня защищенности ИСПДн;

формирования обоснованных требований по обеспечению безопасности ПДн. Под угрозами безопасности ПДн при их обработке в ИСПДн понимается совокупность условий и факторов, создающих потенциальную или реально существующую опасность, связанную с утечкой информации и (или) несанкционированными и (или) непреднамеренными воздействиями на нее.

Модель нарушителя, с учетом которой разрабатывалась модель угроз безопасности ПДн, приведена в Приложении А.

Угрозы безопасности информации определяются по результатам оценки возможностей (потенциала, оснащенности и мотивации) внешних и внутренних нарушителей, анализа возможных уязвимостей информационной системы, возможных способов реализации угроз безопасности информации и последствий от нарушения свойств безопасности информации (конфиденциальности, целостности, доступности).

При определении угроз безопасности информации учитываются структурно-функциональные характеристики информационной системы, включающие структуру и состав информационной системы, физические, логические, функциональные и технологические взаимосвязи между сегментами информационной системы, с иными информационными системами и информационно-телекоммуникационными сетями, режимы обработки информации в информационной системе и в ее отдельных сегментах, а также иные характеристики информационной системы, применяемые информационные технологии и особенности ее функционирования.

По результатам определения угроз безопасности информации при необходимости разрабатываются рекомендации по корректировке структурно-функциональных характеристик информационной системы, направленные на блокирование (нейтрализацию) отдельных угроз безопасности информации.

Модель угроз безопасности информации должна содержать описание информационной системы и ее структурно-функциональных характеристик, а также описание угроз безопасности информации, включающее описание возможностей нарушителей (модель нарушителя), возможных уязвимостей информационной системы, способов реализации угроз безопасности информации и последствий от нарушения свойств безопасности информации.

Требования к системе защиты информации информационной системы определяются в зависимости от класса защищенности информационной системы и угроз безопасности информации, включенных в модель угроз безопасности информации.

Требования к системе защиты информации информационной системы включаются в техническое задание на создание информационной системы и (или) техническое задание (частное техническое задание) на создание системы защиты информации информационной системы, разрабатываемые с учетом ГОСТ 34.602, ГОСТ Р 51583 и ГОСТ Р 51624, и должны в том числе содержать:

цель и задачи обеспечения защиты информации в информационной системе;

уровень защищенности информационной системы;

перечень нормативных правовых актов, методических документов и национальных стандартов, которым должна соответствовать информационная система;

перечень объектов защиты информационной системы;

требования к мерам и средствам защиты информации, применяемым в информационной системе;

требования к защите информации при информационном взаимодействии с иными информационными системами и информационно-телекоммуникационными сетями, в том числе с информационными системами уполномоченного лица, а также при применении вычислительных ресурсов (мощностей), предоставляемых уполномоченным лицом для обработки информации.

2. Перечень принятых сокращений

АРМ - Автоматизированное рабочее место
БД - База данных
ИБ - Информационная безопасность
ИС - Информационная система
ГИС – Государственная информационная система
ИСПДн - Информационная система персональных данных
КЗ - Контролируемая зона
НСД - Несанкционированный доступ
ОС - Операционная система
ПДн - Персональные данные
ПО - Программное обеспечение
ПЭМИН - Побочные электромагнитные излучения и наводки
РД - Руководящий документ
СЗ - Средства защиты
ОРД - Организационно-распорядительные документы

3. Принятые термины и определения

В настоящем документе используются следующие термины и их определения.

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

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.

Доступ к информации – возможность получения информации и ее использования.

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

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

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

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

Контролируемая зона – территория объекта, в пределах которой исключено неконтролируемое присутствие посторонних лиц и транспортных средств, не имеющих права постоянного или разового доступа (пропуска). Посторонние лица и транспортные средства, получившие право разового доступа (пропуска) в КЗ, не должны находиться в пределах этой зоны без постоянного наблюдения (сопровождения).

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

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.

Несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных.

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

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

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.

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.

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

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

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

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

Уязвимость – 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).

4. Порядок определения угроз безопасности ПДн

Подход к определению угроз безопасности ПДн при их обработке в ИСПДн соответствует требованиям приказа ФСТЭК России от 18 февраля 2013 года № 21.

4.1. Формирование перечня возможных угроз ПДн

Перечень возможных угроз сформирован на основании следующих документов:

- Федеральным законом Российской Федерации от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральным законом Российской Федерации от 27 июля 2006 года № 152-ФЗ «О персональных данных»;
- Указом Президента Российской Федерации от 17 марта 2008 года № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена»;
- Приказом ФСТЭК России от 18 февраля 2013 года № 21;
- Приказом ФСБ России от 10 июля 2014 г. N 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»;
- РД Гостехкомиссии России «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации;
- РД Гостехкомиссии России «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации»;
- Положением о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005), утвержденным приказом ФСБ России от 9 февраля 2005 г. № 66, зарегистрировано Министерством юстиции Российской Федерации от 3 марта 2005 года № 6382.
- ГОСТ Р 51275-2006 «Защита информации. Факторы, воздействующие на

информацию. Общие положения».

- Постановление Правительства Российской Федерации № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» от 01 ноября 2012 года.

Формирование требований к защите информации, содержащейся в информационной системе, осуществляется обладателем информации (заказчиком).

Формирование требований к защите информации, содержащейся в информационной системе, осуществляется с учетом ГОСТ Р 51583 «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения» (далее - ГОСТ Р 51583) и ГОСТ Р 51624 «Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования» (далее - ГОСТ Р 51624) и в том числе включает:

принятие решения о необходимости защиты информации, содержащейся в информационной системе;

определение уровня защищенности информационной системы;

определение угроз безопасности информации, реализация которых может привести к нарушению безопасности информации в информационной системе, и разработку на их основе модели угроз безопасности информации;

определение требований к системе защиты информации информационной системы.

В настоящей модели угроз рассматриваются угрозы безопасности ИСПДн СБИС++, которые могут быть реализованы в ИСПДн.

Организационные и технические меры защиты информации, реализуемые в ИСПДН в рамках ее системы защиты информации, в зависимости от угроз безопасности информации, используемых информационных технологий и структурно-функциональных характеристик СБИС++ должны обеспечивать (согласно требованиям в соответствии с постановлением правительства №1119 Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных):

- организация режима обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;

- обеспечение сохранности носителей персональных данных;

- утверждение руководителем оператора документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей;

- использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз.

Содержание мер по обеспечению безопасности персональных данных (в соответствии с Требованиями приказа «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» от 18 февраля 2013 г. ФСТЭК N 21):

I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)

ИАФ.1 - Идентификация и аутентификация пользователей, являющихся работниками оператора

ИАФ.З - Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов

ИАФ.4- Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации

ИАФ.5-Защита обратной связи при вводе аутентификационной информации.

ИАФ.6-Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей).

II. Управление доступом субъектов доступа к объектам доступа (УПД)

УПД.1 - Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей

УПД.2-Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа

УПД.3-Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами

УПД.4-Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы

УПД.5-Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы

УПД.6-Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе)

УПД.13-Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети

УПД.14-Регламентация и контроль использования в информационной системе технологий беспроводного доступа

УПД.15-Регламентация и контроль использования в информационной системе мобильных технических средств

УПД.16-Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы)

V. Регистрация событий безопасности (РСБ)

РСБ.1- Определение событий безопасности, подлежащих регистрации, и сроков их хранения

РСБ.2-Определение состава и содержания информации о событиях безопасности, подлежащих регистрации

РСБ.3-Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения

РСБ. 7-Защита информации о событиях безопасности

VI. Антивирусная защита (АВЗ)

АВЗ.1-Реализация антивирусной защиты

АВЗ.2-Обновление базы данных признаков вредоносных компьютерных программ (вирусов)

VIII. Контроль (анализ) защищенности персональных данных (АНЗ)

АНЗ.2-Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации

XI. Защита среды виртуализации (ЗСВ)

ЗСВ.1-Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации

ЗСВ.2-Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин

XII. Защита технических средств (ЗТС)

ЗТС.3-Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы, в помещения и сооружения, в которых они установлены

ЗТС.4-Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр

XIII. Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)

ЗИС.3-Обеспечение защиты персональных данных от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи.

4.2. Оценка степени негативных последствий субъектам персональных данных вследствие реализации угроз персональным данным

Непосредственный ущерб субъектам ПДн может проявляться в виде:

причинения неудобств субъектам ПДн;

причинения морального ущерба субъектам ПДн;

недополучения субъектами ПДн ожидаемого дохода, возникновения незапланированных финансовых или материальных затрат;

возникновение юридических последствий, ограничений прав и свобод;

нанесения вреда здоровью субъектам ПДн или создания угрозы жизни.

В настоящей модели угроз применяется следующий подход к определению степени негативных последствий для субъектов ПДн:

1) Негативные последствия для субъектов персональных данных отсутствуют, если в результате реализации угрозы ПДн могут быть причинены неудобства субъектам ПДн, не связанные с нарушением их прав, например, вследствие невозможности оперативной обработки ПДн субъекта по желанию субъекта ПДн.

2) Незначительные негативные последствия для субъектов персональных данных – в результате реализации угрозы оказался скомпрометированным ограниченный объем (состав) извлеченных (выгруженных) из БД ПДн, в отношении которых возможно их незаконное использование (разглашение, искажение), что может повлечь нанесение морального вреда субъектам ПДн вследствие нарушения их неимущественных прав, Негативные последствия также могут считаться незначительными по причине того, что принятие решений, порождающих юридические последствия в отношении субъекта не предусматривается исключительно на основании автоматизированной обработки.

3) Негативные последствия для субъектов персональных данных - в результате реализации угрозы ПДн оказались скомпрометированными обрабатываемые в ИСПДн ПДн, при этом их несанкционированная модификация может породить нежелательные юридические последствия в отношении субъектов ПДн, а также иным образом затронуть их имущественные права и законные интересы.

4) Значительные негативные последствия для субъектов ПДн - в результате реализации угрозы ПДн оказываются скомпрометированными специальные категории ПДн (при наличии в ИСПДн такой информации), что может угрожать здоровью или жизни субъектов ПДн.

4.3. Определение актуальных угроз персональным данным

На первом этапе по результатам анализа исходных данных, собранных в ходе обследования ИСПДн, определяется уровень исходной защищенности ИСПДн, который обозначается коэффициентом Y1.

Под уровнем исходной защищенности ИСПДн понимается обобщенный показатель, зависящий от технических и эксплуатационных характеристик ИСПДн, приведенных в Табл. 1.

Табл. 1 – Показатели исходной защищенности ИСПДн

Технические и эксплуатационные характеристики ИСПДн	**Уровень защищенности**		
	Высокий	**Средний**	**Низкий**
1. По территориальному размещению:			
распределенная ИСПДн, которая охватывает несколько областей, краев, округов или государство в целом;	–	–	+

городская ИСПДн, охватывающая не более одного населенного пункта (города, поселка);	–	–	+
корпоративная распределенная ИСПДн, охватывающая многие подразделения одной организации;	–	-	+
локальная (кампусная) ИСПДн, развернутая в пределах нескольких близко расположенных зданий;	–	-	+
локальная ИСПДн, развернутая в пределах одного здания.	-	–	+
2. По наличию соединения с сетями общего пользования:			
ИСПДн, имеющая многоточечный выход в сеть общего пользования;	–	–	+
ИСПДн, имеющая одноточечный выход в сеть общего пользования;	–	-	+
ИСПДн, физически отделенная от сети общего пользования.	-	–	+
3. По встроенным (легальным) операциям с записями баз персональных данных:			
чтение, поиск;	+	–	–
запись, удаление, сортировка;	–	+	–
модификация, передача	–	–	+
4. По разграничению доступа к персональным данным:			
ИСПДн, к которой имеет доступ определенный перечень сотрудников организации, являющейся владельцем ИСПДн, либо субъект ПДн;	–	-	+
ИСПДн, к которой имеют доступ все сотрудники организации,	–	–	+

являющейся владельцем ИСПДн;			
ИСПДн с открытым доступом.	–	–	+
5. По наличию соединений с другими базами ПДн иных ИСПДн:			
интегрированная ИСПДн (организация использует несколько баз ПДн ИСПДн, при этом организация не является владельцем всех используемых баз ПДн);	–	–	+
ИСПДн, в которой используется одна база ПДн, принадлежащая организации – владельцу данной ИСПДн	-	–	+
6. По уровню обобщения (обезличивания) ПДн: ИСПДн, в которой предоставляемые пользователю данные являются обезличенными (на уровне организации, отрасли, области, региона и т.д.); ИСПДн, в которой данные обезличиваются только при передаче в другие организации и не обезличены при предоставлении пользователю в организации; ИСПДн, в которой предоставляемые пользователю данные не являются обезличенными (т.е. присутствует информация, позволяющая идентифицировать субъекта ПДн).	- – –	– - –	+ + +
7. По объему ПДн, которые предоставляются сторонним пользователям			

ИСПДн без предварительной обработки:			
ИСПДн, предоставляющая всю БД с ПДн;	–	–	+
ИСПДн, предоставляющая часть ПДн;	–	-	+
ИСПДн, не предоставляющие никакой информации.	-	–	+

1) ИСПДн имеет высокий уровень исходной защищенности, если не менее 70% характеристик ИСПДн соответствуют уровню «высокий» (суммируются положительные решения по первому столбцу, соответствующему высокому уровню защищенности), а остальные – среднему уровню защищенности (положительные решения по второму столбцу).

2) ИСПДн имеет средний уровень исходной защищенности, если не выполняются условия по пункту 1 и не менее 70% характеристик ИСПДн соответствуют уровню не ниже «средний» (берется отношение суммы положительных решений по второму столбцу, соответствующему среднему уровню защищенности, к общему количеству решений), а остальные – низкому уровню защищенности.

3) ИСПДн имеет низкую степень исходной защищенности, если не выполняются условия по пунктам 1 и 2.

При составлении перечня актуальных угроз безопасности ПДн каждой степени исходной защищенности ставится в соответствие числовой коэффициент Y_1, а именно:

0 – для высокой степени исходной защищенности;

5 – для средней степени исходной защищенности;

10 – для низкой степени исходной защищенности.

Под частотой (вероятностью) реализации угрозы понимается определяемый экспертным путем показатель, характеризующий, насколько вероятной является реализация конкретной угрозы безопасности ПДн для данной ИСПДн в складывающихся условиях обстановки. Вводятся четыре вербальных градации этого показателя:

маловероятно – отсутствуют объективные предпосылки для осуществления угрозы (например, угроза хищения носителей информации лицами, не имеющими легального доступа в помещение, где последние хранятся);

маловероятно – отсутствуют объективные предпосылки для осуществления угрозы (например, угроза хищения носителей информации лицами, не имеющими легального доступа в помещение, где последние хранятся);

низкая вероятность – объективные предпосылки для реализации угрозы существуют, но принятые меры существенно затрудняют ее реализацию (например, использованы соответствующие средства защиты информации);

средняя вероятность – объективные предпосылки для реализации угрозы существуют, но принятые меры обеспечения безопасности ПДн недостаточны;

высокая вероятность – объективные предпосылки для реализации угрозы существуют, и меры по обеспечению безопасности ПДн не приняты.

При составлении перечня актуальных угроз безопасности ПДн каждому значению вероятности возникновения угрозы соответствует числовой коэффициент Y_2, а именно:

0 – для маловероятной угрозы;

2 – для низкой вероятности угрозы;

5 – для средней вероятности угрозы;

10 – для высокой вероятности угрозы.

С учетом изложенного, коэффициент реализуемости угрозы Y будет определяться соотношением:

$$Y = (Y1+Y2)/20.$$

По значению коэффициента реализуемости угрозы Y вербальная интерпретация

реализуемости угрозы формируется следующим образом:

если $0 < Y \leq 0,3$, то возможность реализации угрозы признается низкой;

если $0,3 < Y \leq 0,6$, то возможность реализации угрозы признается средней;

если $0,6 < Y \leq 0,8$, то возможность реализации угрозы признается высокой;

если $Y > 0,8$, то возможность реализации угрозы признается очень высокой.

Затем оценивается опасность каждой угрозы. При оценке опасности на основе опроса экспертов определяется показатель (согласно п. 2.2) опасности угрозы для рассматриваемой ИСПДн. Данный показатель может принимать 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.

В завершение осуществляется выбор из общего (предварительного) перечня угроз безопасности тех, которые относятся к актуальным для данной ИСПДн в соответствии с правилами, показанными в Таблице 2.

Таблица 2 – Правила отнесения угрозы безопасности ПДн к актуальной

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

4.4. Экспертные подходы и решения при построении модели угроз

Выбранные и реализованные в СБИС++ в рамках ее системы защиты информации меры защиты информации должны обеспечивать **4й уровень защищенности**.

Технические меры защиты информации реализуются посредством применения средств защиты информации, имеющих необходимые функции безопасности.

Таблица 3 – Состав мер защиты информации и их базовые наборы для соответствующего уровня защищенности ИСПДн СБИС++.

Условное обозначение и номер меры	Меры защиты информации в информационных системах	Класс защищенности информационной системы			
		4	3	2	1
I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)					
ИАФ.1	Идентификация и аутентификация пользователей, являющихся работниками оператора	+			
ИАФ.2	Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных	-			
ИАФ.3	Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов	+			
ИАФ.4	Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации	+			

ИАФ.5	Защита обратной связи при вводе аутентификационной информации	+			
ИАФ.6	Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей)	+			
ИАФ.7	Идентификация и аутентификация объектов файловой системы, запускаемых и исполняемых модулей, объектов систем управления базами данных, объектов, создаваемых прикладным и специальным программным обеспечением, иных объектов доступа				
II. Управление доступом субъектов доступа к объектам доступа (УПД)					
УПД.1	Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей	+			
УПД.2	Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа	+			
УПД.3	Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами	+			
УПД.4	Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы	+			
УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы	+			
УПД.6	Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе)	+			
УПД.7	Предупреждение пользователя при его входе в информационную систему о том, что в информационной системе реализованы меры защиты информации, и о необходимости соблюдения им установленных оператором правил обработки информации	-			
УПД.8	Оповещение пользователя после успешного входа в информационную систему о его предыдущем входе в информационную систему	-			
УПД.9	Ограничение числа параллельных сеансов доступа для каждой учетной записи пользователя информационной системы	-			

УПД.10	Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу	-			
УПД.11	Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации	-			
УПД.12	Поддержка и сохранение атрибутов безопасности (меток безопасности), связанных с информацией в процессе ее хранения и обработки	-			
УПД.13	Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети	+			
УПД.14	Регламентация и контроль использования в информационной системе технологий беспроводного доступа	+			
УПД.15	Регламентация и контроль использования в информационной системе мобильных технических средств	+			
УПД.16	Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы)	+			
УПД.17	Обеспечение доверенной загрузки средств вычислительной техники	-			
III. Ограничение программной среды (ОПС)					
ОПС.1	Управление запуском (обращениями) компонентов программного обеспечения, в том числе определение запускаемых компонентов, настройка параметров запуска компонентов, контроль за запуском компонентов программного обеспечения	-			
ОПС.2	Управление установкой (инсталляцией) компонентов программного обеспечения, в том числе определение компонентов, подлежащих установке, настройка параметров установки компонентов, контроль за установкой компонентов программного обеспечения	-			
ОПС.3	Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов	-			
ОПС.4	Управление временными файлами, в том числе запрет, разрешение, перенаправление записи, удаление временных файлов	-			
IV. Защита машинных носителей информации (ЗНИ)					
ЗНИ.1	Учет машинных носителей информации	-			
ЗНИ.2	Управление доступом к машинным носителям информации	-			

ЗНИ.3	Контроль перемещения машинных носителей информации за пределы контролируемой зоны	-			
ЗНИ.4	Исключение возможности несанкционированного ознакомления с содержанием информации, хранящейся на машинных носителях, и (или) использования носителей информации в иных информационных системах	-			
ЗНИ.5	Контроль использования интерфейсов ввода (вывода) информации на машинные носители информации	-			
ЗНИ.6	Контроль ввода (вывода) информации на машинные носители информации	-			
ЗНИ.7	Контроль подключения машинных носителей информации	-			
ЗНИ.8	Уничтожение (стирание) информации на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания)	-			
V. Регистрация событий безопасности (РСБ)					
РСБ.1	Определение событий безопасности, подлежащих регистрации, и сроков их хранения	+			
РСБ.2	Определение состава и содержания информации о событиях безопасности, подлежащих регистрации	+			
РСБ.3	Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения	+			
РСБ.4	Реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти	-			
РСБ.5	Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них	-			
РСБ.6	Генерирование временных меток и (или) синхронизация системного времени в информационной системе	-			
РСБ.7	Защита информации о событиях безопасности	+			
РСБ.8	Обеспечение возможности просмотра и анализа информации о действиях отдельных пользователей в информационной системе	-			
VI. Антивирусная защита (АВЗ)					
АВЗ.1	Реализация антивирусной защиты	+			

АВЗ.2	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)	+			
VII. Обнаружение вторжений (СОВ)					
СОВ.1	Обнаружение вторжений	-			
СОВ.2	Обновление базы решающих правил	-			
VIII. Контроль (анализ) защищенности информации (АНЗ)					
АНЗ.1	Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей	-			
АНЗ.2	Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации	+			
АНЗ.3	Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации	-			
АНЗ.4	Контроль состава технических средств, программного обеспечения и средств защиты информации	-			
АНЗ.5	Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в информационной системе	-			
IX. Обеспечение целостности информационной системы и информации (ОЦЛ)					
ОЦЛ.1	Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации	-			
ОЦЛ.2	Контроль целостности информации, содержащейся в базах данных информационной системы	-			
ОЦЛ.3	Обеспечение возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций	-			
ОЦЛ.4	Обнаружение и реагирование на поступление в информационную систему незапрашиваемых электронных сообщений (писем, документов) и иной информации, не относящихся к функционированию информационной системы (защита от спама)	-			
ОЦЛ.5	Контроль содержания информации, передаваемой из информационной системы (контейнерный, основанный на свойствах объекта доступа, и контентный, основанный на поиске запрещенной к передаче информации с использованием сигнатур, масок и иных методов), и исключение неправомерной	-			

	передачи информации из информационной системы				
ОЦЛ.6	Ограничение прав пользователей по вводу информации в информационную систему	-			
ОЦЛ.7	Контроль точности, полноты и правильности данных, вводимых в информационную систему	-			
ОЦЛ.8	Контроль ошибочных действий пользователей по вводу и (или) передаче информации и предупреждение пользователей об ошибочных действиях	-			
X. Обеспечение доступности информации (ОДТ)					
ОДТ.1	Использование отказоустойчивых технических средств	-			
ОДТ.2	Резервирование технических средств, программного обеспечения, каналов передачи информации, средств обеспечения функционирования информационной системы	-			
ОДТ.3	Контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование	-			
ОДТ.4	Периодическое резервное копирование информации на резервные машинные носители информации	-			
ОДТ.5	Обеспечение возможности восстановления информации с резервных машинных носителей информации (резервных копий) в течение установленного временного интервала	-			
ОДТ.6	Кластеризация информационной системы и (или) ее сегментов	-			
ОДТ.7	Контроль состояния и качества предоставления уполномоченным лицом вычислительных ресурсов (мощностей), в том числе по передаче информации	-			
XI. Защита среды виртуализации (ЗСВ)					
ЗСВ.1	Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации	+			
ЗСВ.2	Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин	+			
ЗСВ.3	Регистрация событий безопасности в виртуальной инфраструктуре	-			

ЗСВ.4	Управление (фильтрация, маршрутизация, контроль соединения, однонаправленная передача) потоками информации между компонентами виртуальной инфраструктуры, а также по периметру виртуальной инфраструктуры	-			
ЗСВ.5	Доверенная загрузка серверов виртуализации, виртуальной машины (контейнера), серверов управления виртуализацией	-			
ЗСВ.6	Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных	-			
ЗСВ.7	Контроль целостности виртуальной инфраструктуры и ее конфигураций	-			
ЗСВ.8	Резервное копирование данных, резервирование технических средств, программного обеспечения виртуальной инфраструктуры, а также каналов связи внутри виртуальной инфраструктуры	-			
ЗСВ.9	Реализация и управление антивирусной защитой в виртуальной инфраструктуре	-			
ЗСВ.10	Разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки информации отдельным пользователем и (или) группой пользователей	-			
XII. Защита технических средств (ЗТС)					
ЗТС.1	Защита информации, обрабатываемой техническими средствами, от ее утечки по техническим каналам	-			
ЗТС.2	Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования	-			
ЗТС.3	Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы и помещения и сооружения, в которых они установлены	+			
ЗТС.4	Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр	+			
ЗТС.5	Защита от внешних воздействий (воздействий окружающей среды, нестабильности электроснабжения, кондиционирования и иных	-			

	внешних факторов)				
XIII. Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)					
ЗИС.1	Разделение в информационной системе функций по управлению (администрированию) информационной системой, управлению (администрированию) системой защиты информации, функций по обработке информации и иных функций информационной системы	-			
ЗИС.2	Предотвращение задержки или прерывания выполнения процессов с высоким приоритетом со стороны процессов с низким приоритетом	-			
ЗИС.3	Обеспечение защиты информации от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи	+			
ЗИС.4	Обеспечение доверенных канала, маршрута между администратором, пользователем и средствами защиты информации (функциями безопасности средств защиты информации)	-			
ЗИС.5	Запрет несанкционированной удаленной активации видеокамер, микрофонов и иных периферийных устройств, которые могут активироваться удаленно, и оповещение пользователей об активации таких устройств	-			
ЗИС.6	Передача и контроль целостности атрибутов безопасности (меток безопасности), связанных с информацией, при обмене информацией с иными информационными системами	-			
ЗИС.7	Контроль санкционированного и исключение несанкционированного использования технологий мобильного кода, в том числе регистрация событий, связанных с использованием технологий мобильного кода, их анализ и реагирование на нарушения, связанные с использованием технологий мобильного кода	-			
ЗИС.8	Контроль санкционированного и исключение несанкционированного использования технологий передачи речи, в том числе регистрация событий, связанных с использованием технологий передачи речи, их анализ и реагирование на нарушения, связанные с использованием технологий передачи речи	-			
ЗИС.9	Контроль санкционированной и исключение несанкционированной передачи видеоинформации, в том числе регистрация событий, связанных с	-			

	передачей видеоинформации, их анализ и реагирование на нарушения, связанные с передачей видеоинформации				
ЗИС.10	Подтверждение происхождения источника информации, получаемой в процессе определения сетевых адресов по сетевым именам или определения сетевых имен по сетевым адресам	-			
ЗИС.11	Обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов	-			
ЗИС.12	Исключение возможности отрицания пользователем факта отправки информации другому пользователю	-			
ЗИС.13	Исключение возможности отрицания пользователем факта получения информации от другого пользователя	-			
ЗИС.14	Использование устройств терминального доступа для обработки информации	-			
ЗИС.15	Защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки информации	-			
ЗИС.16	Выявление, анализ и блокирование в информационной системе скрытых каналов передачи информации в обход реализованных мер защиты информации или внутри разрешенных сетевых протоколов	-			
ЗИС.17	Разбиение информационной системы на сегменты (сегментирование информационной системы) и обеспечение защиты периметров сегментов информационной системы	-			
ЗИС.18	Обеспечение загрузки и исполнения программного обеспечения с машинных носителей информации, доступных только для чтения, и контроль целостности данного программного обеспечения	-			
ЗИС.19	Изоляция процессов (выполнение программ) в выделенной области памяти	-			
ЗИС.20	Защита беспроводных соединений, применяемых в информационной системе	-			

"+" - мера защиты информации включена в базовый набор мер для соответствующего уровню защищенности ИСПДн.

Меры защиты информации, не обозначенные знаком "+", применяются при адаптации базового набора мер и уточнении адаптированного базового набора мер, а также при разработке компенсирующих мер защиты информации в информационной системе соответствующего класса защищенности.

5. Модель угроз ИСПДн

5.1. Источники угроз

В качестве возможных источников угроз безопасности ПДн в настоящей модели угроз рассматриваются:

внутренние нарушители;

внешние нарушители.

В качестве вероятных внутренних нарушителей рассматриваются пользователи ИСПДн, имеющие легальный доступ к ИСПДн. В качестве вероятных внешних нарушителей рассматриваются злоумышленники, не являющиеся сотрудниками учреждения, и не имеющие свободного доступа в контролируемую зону, а также контрагенты, осуществляющие поддержку ИСПДн.

Подробное описание, характеристика, а также обоснование выбора вероятных внутренних и внешних нарушителей приведены в Модели нарушителя, представленной в Приложении А настоящей Модели угроз.

6. Заключение

К актуальным угрозам ИСПДн СБИС++ относятся:

1) Подбор логина/пароля (внутренние нарушители).

2) Угрозы, реализуемые в ходе загрузки операционной системы и направленные на перехват паролей или идентификаторов, модификацию базовой системы ввода/вывода (BIOS), перехват управления загрузкой (внутренние нарушители).

3) Использование недостатков уязвимостей ПО.

4) Использование недостатков и уязвимостей программного обеспечения.

5) Перехват информации (сетевого трафика).

6) Вынос ПДн за пределы контролируемой зоны на съемном носителе информации (внутренние нарушители).

7) Умышленное неправомерное внесение изменений в ПДн (внутренние нарушители).

8) Неумышленное искажение или удаление ПДн (внутренние нарушители).

9) 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. (внутренние нарушители).

10) Технологические сбои, отказы, аварии систем обеспечения.

11) Утрата, кража ключей и атрибутов доступа (внешние нарушители).

12) Технологические сбои, отказы, аварии СВТ.

13) Неумышленное нарушение нормального функционирования ИСПДн.

14) Внедрение вирусов или иного вредоносного программного кода.

Согласно п. 5 Постановления Правительства Российской Федерации № 1119 ИСПДн является системой, обрабатывающей иные категории персональных данных. Таким образом, согласно п. 10-е Постановления Правительства Российской Федерации № 1119 ИСПДн требует 4-го уровня защищенности персональных данных при их обработке в информационной системе.

Состав и содержание организационных и технических мер, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для 4 уровня защищенности.

а) организация режима обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;

б) обеспечение сохранности носителей персональных данных;

в) утверждение руководителем оператора документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей;

г) использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз.

1. Обеспечение режима, препятствующего возможности неконтролируемого проникновения или пребывания в помещениях, где размещены используемые СКЗИ, хранятся

СКЗИ и (или) носители ключевой, аутентифицирующей и парольной информации СКЗИ (далее - Помещения), лиц, не имеющих права доступа в Помещения, которое достигается путем:

а) оснащения Помещений входными дверьми с замками, обеспечения постоянного закрытия дверей Помещений на замок и их открытия только для санкционированного прохода, а также опечатывания Помещений по окончании рабочего дня или оборудование Помещений соответствующими техническими устройствами, сигнализирующими о несанкционированном вскрытии Помещений;

б) утверждения правил доступа в Помещения в рабочее и нерабочее время, а также в нештатных ситуациях;

в) утверждения перечня лиц, имеющих право доступа в Помещения.

2. Для обеспечения сохранности носителей персональных данных необходимо:

а) осуществлять хранение съемных машинных носителей персональных данных в сейфах (металлических шкафах), оборудованных внутренними замками с двумя или более дубликатами ключей и приспособлениями для опечатывания замочных скважин или кодовыми замками. В случае если на съемном машинном носителе персональных данных хранятся только персональные данные в зашифрованном с использованием СКЗИ виде, допускается хранение таких носителей вне
сейфов (металлических шкафов);

б) осуществлять поэкземплярный учет машинных носителей персональных данных, который достигается путем ведения журнала учета носителей персональных данных с использованием регистрационных (заводских) номеров.

3. Для выполнения требований, указанных в подпункте "в", необходимо:

а) разработать и утвердить документ, определяющий перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей;

б) поддерживать в актуальном состоянии документ, определяющий перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей.

4. Для выполнения требования, указанных в подпункте "г", необходимо для каждого из уровней защищенности персональных данных применение СКЗИ соответствующего класса, позволяющих обеспечивать безопасность персональных данных при реализации целенаправленных действий с использованием аппаратных и (или) программных средств с целью нарушения безопасности защищаемых СКЗИ персональных данных или создания условий для этого (далее - атака), которое достигается путем:

а) получения исходных данных для формирования совокупности предположений о возможностях, которые могут использоваться при создании способов, подготовке и проведении атак;

б) формирования и утверждения руководителем оператора совокупности предположений о возможностях, которые могут использоваться при создании способов, подготовке и проведении атак, и определение на этой основе и с учетом типа актуальных угроз требуемого класса СКЗИ;

в) использования для обеспечения требуемого уровня защищенности персональных данных при их обработке в информационной системе СКЗИ класса КС1 и выше.

В составе ИСПДН СБИС++ применяются СКЗИ КС1 (Крипто-Про).

Приложение А Модель нарушителя

А.1 Описание нарушителя

В соответствии с РД ФСТЭК РФ «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» источниками угроз, реализуемых за счет несанкционированного доступа к информационным ресурсам ИСПДн, являются субъекты, действия которых нарушают регламентируемые в ИСПДн правила разграничения доступа к информации.

Этими субъектами могут быть:

1) нарушитель (человек);

2) программно-аппаратная закладка.

Нарушителем является физическое лицо или группа лиц, случайно или преднамеренно совершающие действия, следствием которых является нарушение безопасности ПДн при их обработке техническими средствами в ИСПДн.

С точки зрения наличия прав легального доступа в помещения, в которых размещены аппаратные средства ИСПДн, нарушители подразделяются на два типа:

1) внутренние нарушители – нарушители, имеющие право санкционированного доступа в контролируемую зону;

2) внешние нарушители – нарушители, не имеющие права санкционированного доступа в пределы контролируемой зоны.

А.1.1 Возможный внутренний нарушитель

Исходя из способа осуществления доступа к ресурсам ИСПДн, а также уровня возможностей, предоставляемых штатными средствами ИСПДн, полномочий, предоставляемых для работы, и квалификации сотрудников, к числу возможных внутренних нарушителей могут относиться:

администраторы ИСПДн;

пользователи ИСПДн;

обслуживающий персонал учреждения.

Администраторы ИСПДн

Данные лица являются пользователями с административными привилегиями. К этой категории относятся системные и сетевые администраторы.

Администраторы ИСПДн имеют полный физический доступ ко всем техническим и программным средствам ИСПДн и обладают правами настройки данных технических средств и ПО.

Пользователи ИСПДн

Данные лица являются зарегистрированными пользователями ИСПДн и имеют санкционированный доступ к комплексу программно-технических средств ИСПДн на своих рабочих местах. При этом физический доступ к системообразующему оборудованию ИСПДн (серверы, сетевое оборудование) для них запрещен. Пользователи имеют доступ к ресурсам ИСПДн и для них не реализованы правила разграничения и контроля сетевого взаимодействия.

Обслуживающий персонал

К обслуживающему персоналу относятся такие лица, как рабочие подсобных помещений, уборщицы и т.п. При этом обслуживающий персонал не является зарегистрированными пользователями ИСПДн и не имеет санкционированного доступа к комплексу программно-технических средств.

А.1.1 Возможный внешний нарушитель

К внешним нарушителям относятся лица, не являющиеся сотрудниками учреждения, бесконтрольное пребывание которых в помещениях с оборудованием ИСПДн невозможно за исключением случаев нарушения внутренних инструкций и случаев преступной или террористической деятельности. Внешними нарушителями также могут быть сотрудники контрагентов, осуществляющих поддержку ИСПДн. Внешние нарушители чаще всего действуют удаленно, а основными угрозами выступают угрозы генерации сетевых атак на ИСПДн, внедрения вредоносных программ, а также перехвата информации в процессе ее передачи по открытым каналам информационного взаимодействия (перехват и анализ сетевого трафика). При этом реализованная система защиты информации значительно затрудняет возможности внешнего нарушителя по изучению функциональных особенностей работы ИСПДн и процессов, связанных с передачей защищаемой информации, а также о структуре и функционировании средств защиты информации.

А.2 Предположение о квалификации возможных нарушителей

А.2.1 Возможный внутренний нарушитель

Администраторы ИСПДн

Администраторы ИСПДн являются высококвалифицированными специалистами в области использования технических средств перехвата информации, а также программных средств анализа сетевого трафика, сканирования устройств, подключенных к сети. Имеют достаточную квалификацию и возможность (привилегии доступа) для осуществления любых видов атак на любые компоненты ИСПДн (серверы, сетевое оборудование, АРМ). Администраторы ИСПДн обладают полной информацией об используемом в информационной среде ИСПДн системном и прикладном ПО.

Пользователи ИСПДн

Пользователи ИСПДн потенциально могут обладать знаниями в области информационных технологий, а также могут иметь достаточную квалификацию для осуществления сканирования ресурсов сети, анализа сетевого трафика и генерации различных типов сетевых атак. Они обладают необходимыми атрибутами (логин/пароль или цифровой сертификат), обеспечивающими доступ к защищаемой информации.

Обслуживающий персонал

Обслуживающий персонал не имеет санкционированного доступа непосредственно к информационной среде ИСПДн (интерфейсы используемого ПО), однако может получить временный доступ к ее техническим средствам. Обслуживающий персонал не обладает достаточными знаниями в области информационных технологий для проведения эффективных атак.

А.2.2 Возможный внешний нарушитель

Внешний нарушитель является квалифицированным специалистом в области сканирования ресурсов сети, анализа сетевого трафика и генерации различных типов сетевых атак, в том числе и с использованием нестандартных протоколов. Нарушитель имеет достаточную квалификацию для генерации атак на интересующие ресурсы ИСПДн и средства защиты информации и может использовать свободно распространяемое ПО и СВТ.

А.3 Выводы о вероятных нарушителях для ИСПДн

Исходя из приведенного описания возможных нарушителей и их квалификации, можно определить вероятных нарушителей для ИСПДн.

Рассматривая администраторов ИСПДн в качестве вероятных нарушителей, необходимо принимать во внимание тот факт, что администраторы назначаются из числа особо проверенных и доверенных лиц. Количество администраторов ИСПДн по сравнению с числом пользователей ИСПДн мало, что позволяет, во-первых, осуществлять эффективный контроль за их деятельностью, во-вторых, надлежаще мотивировать их на надлежащее выполнение служебных обязанностей.

К администраторам ИСПДн применяются организационные меры, включающие кадровые, административные и режимные.

Кадровые меры реализуются осуществлением жесткого отбора кандидатов на должность администратора ИСПДн в соответствии с требованиями внутренних регламентирующих документов.

Деятельность администраторов ИСПДн регламентирована, обязанности закреплены в должностных инструкциях, результаты и качество работы периодически контролируются.

Режимные меры реализуются за счет контроля действий администраторов ИСПДн со стороны Менеджера по аудиту информационной безопасности .

Реализация перечисленных выше организационных мер позволяют не рассматривать администраторов ИСПДн в качестве вероятных нарушителей.

Рассматривая пользователей ИСПДн в качестве вероятных нарушителей необходимо принимать во внимание, что, с одной стороны, к пользователям применяется тот же набор организационных мер, что и к администраторам ИСПДн, однако, недостаточный уровень.

контроля за действиями пользователей, имеющих широкие полномочия, а также сравнительно невысокая мотивация сотрудников низшего исполнительского звена, позволяют рассматривать пользователей ИСПДн в качестве вероятных нарушителей.

Рассматривая обслуживающий персонал в качестве вероятных нарушителей, можно констатировать, что реализованные физические меры разграничения доступа, а также невысокая квалификация таких лиц позволяют не рассматривать обслуживающий персонал в качестве вероятных нарушителей для ИСПДн.

Рассматривая внешних нарушителей в качестве вероятных нарушителей для ИСПДн, необходимо принимать во внимание, что число таких лиц велико, квалификация их в целом также высока. Реализованные меры защиты периметра не исключают возможности проведения атак с использованием вредоносных программ, а также иных методик, направленных на использование недостатков используемого программного обеспечения. Учитывая высокую мотивированность внешних нарушителей, а также недостаточно развитую правовую базу административного и уголовного делопроизводства, можно рассматривать данную категорию лиц в качестве вероятных нарушителей.

Таким образом, в качестве вероятных нарушителей для ИСПДн можно рассматривать:

- пользователей ИСПДн;

- внешних нарушителей.