Приложение № 2
УТВЕРЖДЕНА
распоряжением председателя
Заречной городской территориальной
избирательной комиссии
от 05.03.2025 г. № 01-05/5

ПОЛИТИКА
информационной безопасности при работе с персональными данными в Заречной городской территориальной избирательной комиссии

ОПРЕДЕЛЕНИЯ

В настоящем документе используются следующие термины и их определения.

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

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

Безопасность персональных данных - состояние защищенности персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных.

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

Блокирование персональных данных - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

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

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

Вспомогательные технические средства и системы - технические средства и системы, не предназначенные для передачи, обработки и хранения персональных

данных, устанавливаемые совместно с техническими средствами и системами, предназначенными для обработки персональных данных или в помещениях, в которых установлены информационные системы персональных данных.

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

Доступ к информации - возможность получения информации и ее использования.

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

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

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

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

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

Информационная система персональных данных (ИСПДн) - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

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

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

Контролируемая зона - пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств.

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

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

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

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

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

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

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

Обезличивание персональных данных - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

Обработка персональных данных - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение,

предоставление, доступ), обезличивание, блокирование, удаление, 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, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

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 буквенноцифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации, применяемые в информационных системах.

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

Персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

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

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

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

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

Программная закладка - код программы, преднамеренно внесенный в

программу с целью осуществить утечку, изменить, блокировать, уничтожить информацию или уничтожить и модифицировать программное обеспечение 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 раскрытие персональных данных неопределенному кругу лиц.

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

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

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

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

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

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

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

Уничтожение персональных данных - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (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).

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

АВС - антивирусные средства
АРМ - автоматизированное рабочее место
ВТСС - вспомогательные технические средства и системы
ИСПДн - информационная система персональных данных
КЗ - контролируемая зона
ЛВС - локальная вычислительная сеть
МЭ - межсетевой экран
НСД- несанкционированный доступ
ОС - операционная система
ПДн - персональные данные
ПМВ - программно-математическое воздействие
ПО - программное обеспечение
ПЭМИН - побочные электромагнитные излучения и наводки
САЗ - система анализа защищенности
СЗИ - средства защиты информации
СЗПДн - система (подсистема) защиты персональных данных
СОВ - система обнаружения вторжений
ТКУИ - технические каналы утечки информации
УБПДн - угрозы безопасности персональных данных

ВВЕДЕНИЕ

Настоящая Политика информационной безопасности при работе с персональными данными в Заречной городской территориальной избирательной комиссии (далее - Политика) является официальным документом.

Политика разработана в соответствии с требованиями, установленными:

Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»;

постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

постановлением Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

постановлением Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»;

приказом 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»,

приказом ФСБ России от 10.07.2014 № 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»;

Методическими рекомендациями по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности, утвержденными руководством 8 Центра ФСБ России 31.03.2015 № 149/7/2/6-432.

В Политике определены требования к персоналу ИСПДн, степень ответственности персонала, структура и необходимый уровень защищенности, статус и должностные обязанности сотрудников, ответственных за обеспечение безопасности персональных данных в ИСПДн Заречной городской

территориальной избирательной комиссии (далее – Комиссия).

1. Общие положения

Целью настоящей Политики является обеспечение безопасности объектов защиты Комиссии от всех видов угроз, внешних и внутренних, умышленных и непреднамеренных, минимизация ущерба от возможной реализации угроз безопасности ПДн (УБПДн).

Безопасность персональных данных достигается путем исключения 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.

Информация и связанные с ней ресурсы должны быть доступны для авторизованных пользователей. Должно осуществляться своевременное обнаружение и реагирование на УБПДн.

Должно осуществляться предотвращение преднамеренных или случайных, частичных или полных несанкционированных модификаций или уничтожения данных.

Состав объектов защиты представлен в «Перечне персональных данных, обрабатываемых в Заречной городской территориальной избирательной комиссии в связи с реализацией служебных (трудовых) отношений, а также осуществлением государственных функций».

Состав ИСПДн подлежащих защите, представлен в «Перечне информационных систем персональных данных в Заречной городской территориальной избирательной комиссии».

2. Область действия

Требования настоящей Политики распространяются на всех сотрудников Комиссии (штатных, временных, работающих по контракту и т.п.), а также всех прочих лиц (подрядчики, аудиторы и т.п.).

3. Система защиты персональных данных

Обеспечение безопасности персональных данных достигается, в частности:

определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;

применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;

учетом машинных носителей персональных данных;

обнаружением фактов несанкционированного доступа к персональным данным и принятием мер, в том числе мер по обнаружению, предупреждению и ликвидации последствий компьютерных атак на информационные системы персональных данных и по реагированию на компьютерные инциденты в них;

восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

установлением правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных;

контролем за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.

Система защиты персональных данных (СЗПДн), строится на основании:

Акта внутреннего контроля соответствия обработки персональных данных.

Перечня персональных данных, обрабатываемых в Заречной городской территориальной избирательной комиссии в связи с реализацией служебных (трудовых) отношений, а также осуществлением государственных функций;

Актов классификации информационных систем персональных данных;

Модели угроз безопасности персональных данных;

Матрицы доступа пользователей к защищаемым информационным ресурсам ИСПДн;

Руководящих документов ФСТЭК России и ФСБ России.

На основании этих документов определяется необходимый уровень защищенности ПДн каждой ИСПДн Комиссии. На основании анализа актуальных угроз безопасности ПДн описанного в Модели угроз, делается заключение о необходимости использования технических средств и организационных мероприятий для обеспечения безопасности ПДн. Выбранные необходимые мероприятия отражаются в «Составе мер защиты информационных систем персональных данных».

Для ИСПДн должен быть составлен список используемых технических средств защиты (далее - Список), а так же программного обеспечения, участвующего в обработке ПДн, на всех элементах ИСПДн:

АРМ пользователей;

Сервера приложений;

СУБД;

Границы ЛВС;

Каналов передачи в сети общего пользования и (или) международного обмена, если по ним передаются ПДн.

В зависимости от уровня защищенности ИСПДн и актуальных угроз, СЗПДн может включать следующие технические средства:

антивирусные средства для рабочих станций пользователей и серверов;

средства межсетевого экранирования;

средства криптографической защиты информации при передаче защищаемой информации по каналам связи.

Так же в список должны быть включены функции защиты, обеспечиваемые штатными средствами обработки ПДн операционными системами (ОС), прикладным ПО и специальными комплексами, реализующими средства защиты. Список функций защиты может включать:

управление и разграничение доступа пользователей;

регистрацию и учет действий с информацией;

обеспечение целостности данных;

обнаружение вторжений.

Список используемых технических средств отражается в «Плане мероприятий по обеспечению защиты персональных данных». Список используемых средств должен поддерживаться в актуальном состоянии. При изменении состава технических средств защиты или элементов ИСПДн соответствующие изменения должны быть внесены в Список и утверждены председателем Избирательной комиссии Свердловской области или лицом, ответственным за обеспечение защиты ПДн.

4. Требования к подсистемам СЗПДн

СЗПДн включает в себя следующие подсистемы:

управления доступом, регистрации и учета;

обеспечения целостности и доступности;

антивирусной защиты;

межсетевого экранирования;

анализа защищенности;

обнаружения вторжений;

криптографической защиты.

Подсистемы СЗПДн имеют различный функционал в зависимости от класса ИСПДн, определенного в «Акте классификации информационной системы персональных данных». Список соответствия функций подсистем СЗПДн классу защищенности представлен в техническом задании по созданию системы защиты информации информационной системы персональных данных.

Подсистема управления доступом, регистрации и учета

Подсистема управления доступом, регистрации и учета предназначена для реализации следующих функций:

идентификации и проверки подлинности субъектов доступа при входе в ИСПДн;

идентификации терминалов, узлов сети, каналов связи, внешних устройств по логическим именам;

идентификации программ, томов, каталогов, файлов, записей, полей записей по именам;

регистрации входа (выхода) субъектов доступа в систему (из системы), либо регистрации загрузки и инициализации операционной системы и ее останова.

регистрации попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам;

регистрации попыток доступа программных средств к терминалам, каналам связи, программам, томам, каталогам, файлам, записям, полям записей.

Подсистема управления доступом может быть реализована с помощью штатных средств обработки ПДн (операционных систем, приложений и СУБД). Так же может быть внедрено специальное техническое средство или их комплекс, осуществляющие дополнительные меры по аутентификации и контролю. Например, применение единых хранилищ учетных записей пользователей и регистрационной информации, использование биометрических и технических (с помощью электронных пропусков) мер аутентификации и других.

Подсистема обеспечения целостности и доступности

Подсистема обеспечения целостности и доступности предназначена для обеспечения целостности и доступности ПДн, программных и аппаратных средств ИСПДн Комиссии, а так же средств защиты, при случайной или намеренной модификации.

Подсистема реализуется с помощью организации резервного копирования обрабатываемых данных, а так же резервированием ключевых элементов ИСПДн.

Подсистема антивирусной защиты

Подсистема антивирусной защиты предназначена для обеспечения антивирусной защиты серверов и АРМ пользователей ИСПДн Комиссии.

Средства антивирусной защиты предназначены для реализации следующих функций:

резидентный антивирусный мониторинг;

антивирусное сканирование;

скрипт-блокирование;

централизованной/удаленной установки/деинсталляции антивирусного продукта, настройки, администрирования, просмотра отчетов и статистической информации по работе продукта;

автоматизированного обновления антивирусных баз;

ограничения прав пользователя на остановку исполняемых задач и изменения настроек антивирусного программного обеспечения;

автоматического запуска непосредственно после загрузки операционной системы.

Подсистема реализуется путем внедрения специального антивирусного программного обеспечения на все элементы ИСПДн.

Подсистема межсетевого экранирования

Подсистема межсетевого экранирования предназначена для реализации следующих функций:

фильтрации открытого и зашифрованного (закрытого) IP- трафика;

фиксации во внутренних журналах информации о проходящем открытом и закрытом IP-трафике;

идентификации и аутентификации администратора межсетевого экрана при его локальных запросах на доступ;

регистрации входа (выхода) администратора межсетевого экрана в систему (из системы) либо загрузки и инициализации системы и ее программного останова;

контроля целостности своей программной и информационной части;

фильтрации пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств;

фильтрации с учетом входного и выходного сетевого интерфейса как средства проверки подлинности сетевых адресов;

регистрации и учета запрашиваемых сервисов прикладного уровня;

блокирования доступа неидентифицированного объекта или субъекта, подлинность которого при аутентификации не подтвердилась, методами, устойчивыми к перехвату;

контроля за сетевой активностью приложений и обнаружения сетевых атак.

Подсистема реализуется внедрением программно-аппаратных комплексов межсетевого экранирования на границе ЛВС, классом не ниже 4.

Подсистема анализа защищенности

Подсистема анализа защищенности должна обеспечивать выявление уязвимостей, связанных с ошибками в конфигурации ПО ИСПДн, которые могут быть использованы нарушителем для реализации атаки на систему.

Функционал подсистемы может быть реализован программными и программно-аппаратными средствами.

Подсистема обнаружения вторжений

Подсистема обнаружения вторжений должна обеспечивать выявление сетевых атак на элементы ИСПДн, подключенные к сетям общего пользования и

(или) международного обмена.

Функционал подсистемы может быть реализован программными и программно-аппаратными средствами.

Подсистема криптографической защиты

Подсистема криптографической защиты предназначена для исключения НСД к защищаемой информации в ИСПДн Комиссии при ее передаче по каналам связи сетей общего пользования и (или) международного обмена.

Подсистема реализуется путем внедрения криптографических программно-аппаратных комплексов.

5. Пользователи ИСПДн

В ИСПДн Комиссии можно выделить следующие группы пользователей, участвующих в обработке и хранении ПДн:

Администраторы ИСПДн;

Администраторы безопасности;

Операторы АРМ;

Администраторы сети ИСПДн;

Технические специалисты по обслуживанию периферийного оборудования.

Данные о группах пользователях, уровне их доступа и информированности должны быть отражены в Матрице доступа пользователей к защищаемым информационным ресурсам.

Администратор ИСПДн

Администратор ИСПДн, сотрудник Комиссии (или иное уполномоченное лицо), ответственный за настройку, внедрение и сопровождение ИСПДн. Обеспечивает функционирование подсистемы управления доступом ИСПДн и уполномочен осуществлять предоставление и разграничение доступа конечного пользователя (Оператора АРМ) к элементам, хранящим персональные данные.

Администратор ИСПДн обладает следующим уровнем доступа и знаний:

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.

Администратор безопасности

Администратор безопасности, сотрудник Комиссии (или иное уполномоченное лицо), ответственный за функционирование СЗПДн, включая обслуживание и настройку административной, серверной и клиентской компонент.

Администратор безопасности обладает следующим уровнем доступа и знаний:

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).

Администратор безопасности уполномочен:

реализовывать политики безопасности в части настройки СКЗИ, межсетевых экранов и систем обнаружения атак, в соответствии с которыми пользователь (Оператор АРМ) получает возможность работать с элементами ИСПДн;

осуществлять аудит средств защиты;

Оператор АРМ

Оператор АРМ - сотрудник Комиссии (или иное уполномоченное лицо), осуществляющий обработку ПДн. Обработка ПДн включает: возможность просмотра ПДн, ручной ввод ПДн в систему ИСПДн, формирование справок и отчетов по информации, полученной из ИСПД. Оператор не имеет полномочий для управления подсистемами обработки данных и СЗПДн.

Оператор ИСПДн обладает следующим уровнем доступа и знаний:

обладает всеми необходимыми атрибутами (например, паролем), обеспечивающими доступ к некоторому подмножеству ПДн;

располагает конфиденциальными данными, к которым имеет доступ.

Администратор сети ИСПДн

Администратор сети ИСПДн, сотрудник Комиссии (или иное уполномоченное лицо), ответственный за функционирование телекоммуникационной подсистемы ИСПДн. Администратор сети не имеет полномочий для управления подсистемами обработки данных и безопасности.

Администратор сети обладает следующим уровнем доступа и знаний:

обладает частью информации о системном и прикладном программном обеспечении ИСПДн;

обладает частью информации о технических средствах и конфигурации ИСПДн;

имеет физический доступ к техническим средствам обработки информации и средствам защиты;

знает, по меньшей мере, одно легальное имя доступа.

Технический специалист по обслуживанию периферийного оборудования

Технический специалист по обслуживанию, сотрудник Комиссии (или иное уполномоченное лицо), осуществляет обслуживание и настройку периферийного оборудования ИСПДн. Технический специалист по обслуживанию не имеет доступа к ПДн, не имеет полномочий для управления подсистемами обработки данных и безопасности.

Технический специалист по обслуживанию обладает следующим уровнем доступа и знаний:

обладает частью информации о системном и прикладном программном обеспечении ИСПДн;

обладает частью информации о технических средствах и конфигурации ИСПДн;

знает, по меньшей мере, одно легальное имя доступа.

6. Требования к персоналу по обеспечению защиты ПДн

Все сотрудники Комиссии, являющиеся пользователями ИСПДн, должны четко знать и строго выполнять установленные правила и обязанности по доступу к защищаемым объектам и соблюдению принятого режима безопасности ПДн.

При вступлении в должность нового сотрудника он должен быть ознакомлен с необходимыми документами, регламентирующими требования по защите ПДн, а также обучение навыкам выполнения процедур, необходимых для санкционированного использования ИСПДн.

Сотрудник должен быть ознакомлен со сведениями настоящей Политики, принятых процедур работы с элементами ИСПДн и СЗПДн.

Сотрудники Комиссии, использующие технические средства аутентификации, должны обеспечивать сохранность идентификаторов (электронных ключей) и не допускать НСД к ним, а так же возможность их утери или использования третьими лицами. Пользователи несут персональную ответственность за сохранность идентификаторов.

Сотрудники Комиссии должны следовать установленным процедурам поддержания режима безопасности ПДн при выборе и использовании паролей (если не используются технические средства аутентификации).

Сотрудники Комиссии должны обеспечивать надлежащую защиту оборудования, оставляемого без присмотра, особенно в тех случаях, когда в помещение имеют доступ посторонние лица. Все пользователи должны знать требования по безопасности ПДн и процедуры защиты оборудования, оставленного без присмотра, а также свои обязанности по обеспечению такой защиты.

Сотрудникам запрещается устанавливать постороннее программное обеспечение, подключать личные мобильные устройства и носители информации, а так же записывать на них защищаемую информацию.

Сотрудникам запрещается разглашать защищаемую информацию, которая

стала им известна при работе с информационными системами Комиссии, третьим лицам.

При работе с ПДн в ИСПДн сотрудники Комиссии обязаны обеспечить отсутствие возможности просмотра ПДн третьими лицами с мониторов АРМ или терминалов.

При завершении работы с ИСПДн сотрудники обязаны защитить АРМ или терминалы с помощью блокировки ключом или эквивалентного средства контроля, например, доступом по паролю, если не используются более сильные средства защиты.

Сотрудники Комиссии должны быть проинформированы об угрозах нарушения режима безопасности ПДн и ответственности за его нарушение. Они должны быть ознакомлены с утвержденной формальной процедурой наложения дисциплинарных взысканий на сотрудников, которые нарушили принятые политику и процедуры безопасности ПДн.

Сотрудники обязаны без промедления сообщать обо всех наблюдаемых или подозрительных случаях работы ИСПДн, могущих повлечь за собой угрозы безопасности ПДн, а также о выявленных ими событиях, затрагивающих безопасность ПДн, руководству подразделения и лицу, отвечающему за немедленное реагирование на угрозы безопасности ПДн.

Должностные обязанности пользователей ИСПДн

Должностные обязанности пользователей ИСПДн описаны в следующих документах:

Инструкция администратора ИСПДн;

Инструкция администратора безопасности ИСПДн;

Инструкция пользователя ИСПДн;

Инструкция пользователя при возникновении внештатных ситуаций;

Ответственность сотрудников

В соответствии со статьей 24 Федерального закона Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных» лица, виновные в нарушении требований данного Федерального закона, несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.

Действующее законодательство Российской Федерации позволяет предъявлять требования по обеспечению безопасной работы с защищаемой информацией и предусматривает ответственность за нарушение установленных правил эксплуатации ЭВМ и систем, неправомерный доступ к информации, если эти действия привели к уничтожению, блокированию, модификации информации или нарушению работы ЭВМ или сетей (статьи 272,273 и 274 Уголовного кодекса Российской Федерации).

Администратор ИСПДн и администратор безопасности несут ответственность за все действия, совершенные от имени их учетных записей или системных учетных записей, если не доказан факт несанкционированного использования учетных записей.

При нарушениях сотрудниками Комиссии – пользователями ИСПДн правил, связанных с безопасностью ПДн, они несут ответственность, установленную действующим законодательством Российской Федерации.

7. Список использованных источников

Основными нормативно-правовыми и методическими документами, на которых базируется настоящая Политика, являются:

Федеральный Закон от 27.07.2006 г. № 152-ФЗ «О персональных данных», устанавливающий основные принципы и условия обработки ПДн, права, обязанности и ответственность участников отношений, связанных с обработкой ПДн.

Требования к защите персональных данных при их обработке в информационных системах персональных данных, утвержденные постановлением Правительства Российской Федерации от 01.11.2012 г. № 1119.

Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утвержденное постановлением Правительства Российской Федерации от 15.09.2008 г. № 687.

Нормативно-методические документы Федеральной службы по техническому и экспертному контролю Российской Федерации (далее – ФСТЭК России) по обеспечению безопасности ПДн при их обработке в ИСПДн:

Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденная заместителем директора ФСТЭК России 15.02.2008 г.

Методический документ. Методика оценки угроз безопасности информации, утвержденный ФСТЭК России 05.02.2021 г.

Приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющих государственную тайну, содержащихся в государственных информационных системах».

Приказ 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».

Приказ Федеральной службы безопасности Российской Федерации от 10.07.2014 № 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».

Методические рекомендации по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности, утвержденные руководством 8 Центра ФСБ России 31.03.2015 № 149/7/2/6-432.

Приложение № 3
УТВЕРЖДЕНА
распоряжением председателя
Заречной городской территориальной
избирательной комиссии
от 05.03.2025 г. № 01-05/5

ИНСТРУКЦИЯ
о порядке резервного копирования и восстановления информации в информационных системах персональных данных Заречной городской территориальной избирательной комиссии

Инструкция о порядке резервного копирования и восстановления информации в информационных системах персональных данных Заречной городской территориальной избирательной комиссии регламентирует организационно-техническое обеспечение процессов резервного копирования и восстановления информации в информационных системах персональных данных Заречной городской территориальной избирательной комиссии.

1. Общие положения

1. Инструкция о порядке резервного копирования и восстановления информации в информационных системах персональных данных Заречной городской территориальной избирательной комиссии (далее – Инструкция) является одним из локальных правовых актов Заречной городской территориальной избирательной комиссии (далее – Комиссия) регламентирующих деятельность Комиссии по обеспечению безопасности персональных данных работников организации, участников избирательного процесса, иных лиц, чьи персональные данные могут собираться, храниться и обрабатываться в автоматизированных системах обработки персональных данных (далее – ИСПДн) Комиссии.

2. Настоящая Инструкция разработана в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», другими нормативными правовыми актами по обеспечению безопасности персональных данных и регламентирует организационно-техническое обеспечение процессов резервного копирования и восстановления данных, хранящихся в ИСПДн Комиссии.

3. Настоящая Инструкция разработана с целью:

1) определения категории информации, подлежащей обязательному резервному копированию;

2) определения процедуры резервирования данных для последующего восстановления работоспособности информационных систем при полной или частичной потере информации, вызванной сбоями или отказами аппаратного или программного обеспечения, ошибками пользователей, чрезвычайными обстоятельствами (пожаром, стихийными бедствиями и т.д.);

3) определения порядка восстановления информации в случае возникновения такой необходимости;

4) упорядочения работы и определения ответственности должностных лиц, связанной с резервным копированием и восстановлением информации.

4. Организационное и техническое обеспечение процессов резервного копирования и восстановления данных, хранящихся в ИСПДн Комиссии, а также контроль за действиями исполнителей и обслуживающего персонала при работе с паролями возлагается на Администратора информационных систем персональных данных Комиссии (далее – Администратор ИСПДн).

2. Общие требования к резервному копированию

5. Резервное копирование информации - создание копий защищаемой информации в электронном виде для быстрого восстановления работоспособности ИСПДн в случае возникновения аварийной ситуации, повлекшей за собой повреждение или утрату данных.

6. Резервному копированию подлежит информация следующих категорий:

1) персональная информация пользователей (личные каталоги) и групповая информация (общие каталоги подразделений) на файловых серверах;

2) информация, обрабатываемая пользователями в ИСПДн, а также информация, необходимая для восстановления работоспособности ИСПДн.

7. Резервные копии хранятся на дисковых массивах серверов, находящихся в защищенном серверном помещении, доступ к резервным копиям ограничен средствами разграничения доступа операционной системы.

8. Архивное копирование резервируемой информации производится при помощи специализированных программных систем резервного копирования, обеспечивающих выполнение требований к резервному копированию.

9. Система резервного копирования обеспечивает производительность, достаточную для сохранения информации, в установленные сроки и с заданной периодичностью.

10. Контроль за физическим доступом к оборудованию, на котором осуществляется хранение резервных копий, возлагается на Администратора ИСПДн Комиссии.

3. Ответственность за резервное копирование

11. Ответственность за периодичность и полноту резервного копирования, а также состояние системы резервного копирования возлагается на Администратора ИСПДн Комиссии.

12. Ответственность за контроль над своевременным осуществлением резервного копирования, а также за выполнением требований по хранению архивных копий и предотвращению несанкционированного доступа к ним возлагается на Администратора ИСПДн Комиссии.

13. В случае обнаружения попыток несанкционированного доступа к носителям архивной информации, а также иных нарушениях ИБ, произошедших в процессе резервного копирования, работник, обнаруживший нарушение обязан незамедлительно уведомить Администратора ИСПДн Комиссии.

4. Периодичность резервного копирования, хранение копий

14. Резервное копирование информации производится ежедневно, кроме субботы и воскресенья. Ежедневные копии хранятся в течение нескольких дней до выполнения еженедельного резервного копирования. Еженедельные копии хранятся в течение нескольких недель до выполнения ежемесячного резервного копирования. Ежемесячные копии хранятся не менее трех месяцев.

5. Восстановление информации из резервных копий

15. В случае необходимости восстановление данных из резервных копий производится Администратором ИСПДн Комиссии.

16. Восстановление данных из резервных копий производится в случае их исчезновения или нарушения вследствие несанкционированного доступа в систему, воздействия вирусов, программных ошибок, ошибок работников, аппаратных сбоев, иных причин.

17. Восстановление системного программного обеспечения и программного обеспечения общего назначения производится с их носителей в соответствии с инструкциями производителя.

18. Восстановление специализированного программного обеспечения производится с дистрибутивных носителей или их резервных копий в соответствии с инструкциями по установке или восстановлению данного программного обеспечения.

19. Для восстановления информации используется последняя резервная копия, содержащая необходимые данные в неповрежденном состоянии.

Приложение № 4
УТВЕРЖДЕНА
распоряжением председателя
Заречной городской территориальной
избирательной комиссии
от 05.03.2025 г. № 01-05/5

ИНСТРУКЦИЯ

о порядке учёта, хранения машинных носителей персональных данных в Заречной городской территориальной избирательной комиссии

8. Общие положения

Настоящая Инструкция по порядку учета, хранения машинных носителей персональных данных в Заречной городской территориальной избирательной комиссии (далее – Инструкция) устанавливает порядок учета, хранения и уничтожения съемных носителей и является одним из локальных правовых актов Заречной городской территориальной избирательной комиссии (далее – Комиссия) регламентирующих деятельность Комиссии по обеспечению безопасности персональных данных работников организации, участников избирательного процесса, иных лиц, чьи персональные данные могут собираться, храниться и обрабатываться в автоматизированных системах обработки персональных данных (далее – ИСПДн) Комиссии.

Настоящая инструкция разработана в соответствии с Федеральным законом РФ от 27 июля 2006 года № 149 «Об информации, информационных технологиях и о защите информации», Федеральным законом РФ от 27 июля 2006 года № 152 «О персональных данных», постановлением Правительства Российской Федерации от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», 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».

9. Виды машинных носителей персональных данных

Для обработки (хранения) персональных данных в Комиссии используются следующие типы машинных носителей:

1) съемные носители информации (внешние жесткие магнитные диски, магнитные ленты, USB флеш-накопители, оптические носители (CD, DVD, Blu-ray) и др.);

2) несъемные носители информации (жесткие магнитные диски объектов

информатизации).

В Комиссии допускается использование только учтенных машинных носителей информации, которые подвергаются регулярной ревизии и контролю.

10. Несъемные носители персональных данных

Машинные носители персональных данных, которые располагаются в объекте информатизации (системном блоке, ноутбуке, сервере и т.п.), считаются несъемными машинными носителями.

Корпус объекта информатизации, в котором устанавливаются несъемные машинные носители персональных данных, опечатывается с использованием средств, позволяющих установить несанкционированный доступ к ним (например, с использованием пломбы-наклейки).

Вскрытие опечатанного корпуса объекта информатизации в отсутствии уполномоченных лиц и (или) администратора безопасности (ответственного за обеспечение информационной безопасности) информационной системы персональных данных Комиссии запрещается.

11. Съемные носители персональных данных

Съемные носители персональных данных используются работниками Комиссии для выполнения должностных обязанностей, в том числе для выполнения резервного копирования.

Съемные носители информации выдаются работникам Комиссии в случае возникновения производственной необходимости

12. Учет носителей персональных данных

Учету в Комиссии подлежат все машинные носители персональных данных. Машинные носители должны быть учтены до начала на них хранения (обработки) персональных данных.

Не допускается использование неучтенных машинных носителей персональных данных.

Съемные носители персональных данных маркируются («№_____»).

Общий учет обеспечивает администратор безопасности информационной системы персональных данных (приложение 1).

13. Передача съемных носителей персональных данных

Съемные носители персональных данных после регистрации ответственным за обеспечение защиты персональных данных передаются пользователям под подпись.

В случае увольнения работника предоставленные ему съемные носители изымаются, данные удаляются либо передаются другому работнику.

14. Хранение машинных носителей персональных данных

Съемные носители персональных данных хранятся в опечатываемых запираемых шкафах (сейфах) или в сейфе с ключевым и кодовым замком в соответствии с требованиями к хранению машинных носителей персональных данных, которые перечислены в Положении об обработке и защите персональных данных.

Защита несъемных носителей персональных данных достигается путем опечатывания объектов информатизации, предотвращения несанкционированного доступа в помещения, где они располагаются, в соответствии с Положением об обработке и защите персональных данных.

15. Ответственность

Информация, хранящаяся на съемных носителях, подлежит обязательной проверке на отсутствие вредоносного программного обеспечения перед каждым использованием.

В случае утраты или несанкционированного уничтожения съемных носителей, либо разглашения содержащихся в них сведений немедленно ставится в известность ответственный за обеспечение безопасности персональных данных в информационной системе персональных данных. По факту утраты или уничтожения проводится служебное расследование.

В случае передачи в ремонт съемного носителя все данные на нем должны быть гарантированно удалены в порядке, предусмотренном Положением об обработке и защите персональных данных. Если удалить информацию невозможно, решение о ремонте принимается комиссией по защите персональных данных, при этом с организацией, осуществляющей ремонт, должно быть подписано Соглашение о конфиденциальности.

Передача в ремонт средств вычислительной техники должна проходить без носителей, которые могут содержать персональные данные.

При использовании работниками съемных носителей необходимо:

соблюдать требования настоящей Инструкции;

использовать съемные носители исключительно для выполнения своих должностных обязанностей;

ставить в известность администратора безопасности информационной системы персональных данных Комиссии о любых фактах нарушения требований настоящей Инструкции;

бережно относиться к съемным носителям;

незамедлительно извещать администратора безопасности информационной системы персональных данных Комиссии о фактах утраты (кражи) съемного носителя.

При использовании съемных носителей запрещено:

использовать съемные носители в личных целях;

хранить съемные носители на рабочих столах, либо оставлять их без присмотра или передавать на хранение другим лицам.

Персональную ответственность за сохранность полученных съемных носителей и предотвращение несанкционированного доступа к записанным на них данным несет работник, за которым закреплен носитель.

Все работники Комиссии, обрабатывающие персональные данные, знакомятся под подпись с настоящей инструкцией при информировании о факте обработки персональных данных, категориях обрабатываемых персональных данных, особенностях и правилах такой обработки, установленных нормативными правовыми актами федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, а также локальными правовыми актами Комиссии.

Приложение

к инструкции о порядке учёта, хранения
машинных носителей персональных данных в
Заречной городской территориальной избирательной комиссии

Форма

Журнала учета машинных носителей, содержащих персональные данные

Дата поступления	Регистрационный номер	Откуда поступил	Вид носителя	Кол-во носителей	№ и дата сопроводительного документа	Учтенные номера носителей	Кому передан носитель	Дата передачи носителя	Дата и № акта уничтожения	Ф.И.О.	
										передавшего	получившего
1	2	3	4	5	6	7	8	9	10	11	12

Приложение № 5
УТВЕРЖДЕНА
распоряжением председателя
Заречной городской территориальной
избирательной комиссии
от 05.03.2025 г. № 01-05/5

Модель угроз и нарушителя безопасности персональных данных при их обработке в информационных системах персональных данных Заречной городской территориальной избирательной комиссии

1. Общие положения.

Настоящий документ содержит систематизированный перечень угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Эти угрозы обусловлены преднамеренными или непреднамеренными действиями физических лиц или организаций, а также криминальных группировок, создающих условия (предпосылки) для нарушения безопасности персональных данных (ПДн), которое ведет к ущербу интересов Избирательной комиссии Свердловской области.

Документ предназначен для оценки реализации угроз безопасности ПДн (далее – УБПДн) при их обработке в информационной системе персональных данных (далее – ИСПДн) в Заречной городской территориальной избирательной комиссии (далее – Комиссия). Определение перечня тех угроз и нарушителей информационной безопасности, которые являются актуальными для данных ИСПДн, послужит основой для проведения мероприятий по классификации ИСПДн, проектированию и внедрению системы обеспечения безопасности персональных данных (далее –ПДн) в Комиссии.

В документе рассматриваются все ИСПДн Комиссии, за исключением ИСПДн, связанной с работой комплекса средств автоматизации Государственной автоматизированной системы Российской Федерации «Выборы», эксплуатируемый в Комиссии, поскольку модель угроз и нарушителя безопасности персональных данных при их обработке в Государственной автоматизированной системе Российской Федерации «Выборы» составлена в ФГКУ «Федеральной центр информатизации при Центральной избирательной комиссии Российской Федерации».

При разработке модели угроз безопасности ПДн, обрабатываемых в ИСПДн Избирательной комиссии Свердловской области, в качестве основополагающих, использовались нормативные документы ФСБ и ФСТЭК России, определяющие подходы к безопасности ПДн:

Постановление Правительства №1119 от 1.11.2012 г. «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

Методический документ. Методика оценки угроз безопасности информации, утвержденный ФСТЭК России 05.02.2021 г.;

Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденная заместителем директора ФСТЭК России 15.02.2008 г.;

Приказ ФСБ России № 378 10.07.2014 г «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 уровня защищенности»;

Приказ ФСТЭК РФ от 18 февраля 2013 г. N 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

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

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

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

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

Доступ к информации – возможность получения информации, а также её использования.

Защита персональных данных – комплекс мероприятий, направленных на поддержание целостности, доступности, конфиденциальности информации и ресурсов, используемых для ввода, хранения, обработки и передачи персональных данных.

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.

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.

Комиссия (Оператор, Организация) – Избирательная комиссия Свердловской области.

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-распределённое программное средство (аппаратно-программный комплекс), реализующее контроль информации, поступающей в информационную систему персональных данных и (или) выходящей из информационной системы.

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

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

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

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

Обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Персональные данные – любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных).

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

Пользователь информационной системы персональных данных – лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты её функционирования.

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

Программная закладка – скрытно внесенный в программное обеспечение функциональный объект, который при определенных условиях способен обеспечить несанкционированное программное воздействие. Программная закладка может быть реализована в виде вредоносной программы или программного кода.

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

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

Система защиты персональных данных – система организационных и аппаратно-программных средств, обеспечивающая защиту персональных данных, обрабатываемых в информационной системе персональных данных, от уничтожения, изменения, блокирования, копирования и распространения за счет исключения несанкционированного, в том числе случайного, доступа к персональным данным.

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.

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.

Целостность информации – способность средства вычислительной техники или информационной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

3. Обозначения и сокращения.

В настоящем документе используются следующие обозначения и их сокращения:

ИС – информационная система;

ИСПДн – информационная система персональных данных;

НСД – несанкционированный доступ;

ОС – операционная система;

ПДн – персональные данные;

ПЭМИН – побочные электромагнитные излучения и наводки;

ПО – программное обеспечение;

СФК – среда функционирования криптографических средств;

СКЗИ – средства криптографической защиты информации;

УБПДн – угрозы безопасности персональных данных;

ФСБ России – Федеральная служба безопасности РФ;

ФСТЭК России – Федеральная служба по техническому и экспортному контролю РФ.

4. Характеристики ИСПДн.

4.1. Общая ИСПДн.

В общей ИСПДн Комиссии используется общее программное обеспечение:

- средства операционной системы Microsoft Windows;
- средства продуктов Microsoft Office, Libre Office;
- средства электронной почты в виде веб-клиентов и отдельно стоящих автономных почтовых клиентов.

Характеристики общей ИСПДн представлены в Таблице 1.

Таблица 1.

Характеристика	Значение
Категория обрабатываемых	Иные персональные данные

Характеристика	Значение
персональных данных	
Состав обрабатываемых ПДн	Персональные данные субъектов: - члены Комиссии с правом решающего и совещательного голоса; - члены иных избирательных комиссий, формируемых на территории Свердловской области; - лица, входящие в состав рабочих групп, комиссий, Контрольно-ревизионной службы при Комиссии; - кандидаты, их доверенные лица и уполномоченные представители; - наблюдатели; - уполномоченные представители и доверенные лица избирательных объединений; - члены инициативной группы по проведению референдума Свердловской области, иных групп участников референдума Свердловской области; - лица, привлекаемые Комиссией к административной ответственности за нарушения законодательства о выборах и референдумах, о политических партиях; - участники олимпиад, конкурсов и иных мероприятий, организуемых (проводимых) Комиссией, и их руководители; - лица, представляемые к награждению и поощрению Комиссией; - лица, обратившиеся в Комиссию; - иные категории лиц в соответствии с требованиями законодательства Российской Федерации.
Объем обрабатываемых персональных данных	Менее 100 000
Структура информационной системы	Локальная ИСПДн, развернутая в пределах одного здания
Режим обработки персональных данных	Многопользовательская
Режим разграничения прав доступа пользователей информационной системы	С разграничением прав доступа
Наличие подключения к сетям связи общего пользования и /или сетям международного информационно обмена	Имеется

В соответствии с требованиями к защите персональных данных при обработке в информационных системах персональных данных (утв. постановлением Правительства РФ от 1 ноября 2012 г. № 1119), для Общей ИСПДн актуальны угрозы 3-го типа. При этом ИСПДн обрабатывает специальные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора. Совокупность данных условий требует устанавливать для данной ИСПДн 3 уровень защищенности персональных данных.

5. Модель угроз ИСПДн.

5.1. Принципы построения модели угроз безопасности ПДн.

Построение модели угроз безопасности ПДн основывалось на классификации, анализе и оценки актуальности совокупности условий и факторов, создающих опасность, связанную с утечкой информации и (или) несанкционированными и (или) непреднамеренными воздействиями на нее.

В рамках построения модели угроз безопасности ПДн все вероятные угрозы разделены на две категории:

угрозы безопасности ПДн, реализуемые за счет утечки ПДн по техническим каналам;

угрозы безопасности ПДн, реализуемые за счет несанкционированного доступа (далее – НСД) к ПДн с использованием штатного или специально разработанного программного обеспечения (далее – ПО).

В ходе моделирования идентифицированы все возможные источники угроз, все возможные уязвимости идентифицированы и сопоставлены с идентифицированными источниками угроз, все идентифицированные источники угроз и уязвимости сопоставлены со способами их реализации.

Для всех ИСПДн Комиссии характерны одинаковые угрозы и уязвимости.

5.2. Классификация угроз безопасности ПДн за счёт утечки ПДн по техническим каналам

При обработке ПДн в ИСПДн Комиссии возможно возникновение УБПДн за счет реализации следующих каналов утечки информации по техническому каналу:

угрозы утечки видовой (визуальной) информации;

угрозы утечки информации по каналам побочных электромагнитных излучений и наводок (далее – ПЭМИН).

5.2.1. Угрозы утечки видовой информации.

Источником угроз утечки видовой (визуальной) информации являются физические лица, не имеющие доступа к ИСПДн Комиссии, а также технические средства просмотра, внедренные в служебные помещения или скрытно используемые данными физическими лицами.

Среда распространения информативного сигнала – это физическая среда, по которой информативный сигнал может распространяться – однородная (воздушная).

Угрозы утечки видовой (визуальной) информации реализуются за счет просмотра ПДн с помощью оптических (оптико-электронных) средств с экранов дисплеев и других средств отображения средств вычислительной техники, входящих в состав ИСПДн Комиссии.

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

Источником угроз утечки информации по каналам ПЭМИН являются физические лица, не имеющие доступа к ИСПДн Комиссии.

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

Генерация информации, содержащей ПДн и циркулирующей в технических средствах ИСПДн Комиссии в виде электрических информативных сигналов, ее обработка и передача по электрическим цепям

техническими средствами ИСПДн Комиссии сопровождается побочными электромагнитными излучениями.

Регистрация ПЭМИН осуществляется с целью перехвата информации, циркулирующей в технических средствах, осуществляющих обработку ПДн, путем использования аппаратуры в составе радиоприемных устройств, предназначенной для восстановления информации. Кроме этого, перехват ПЭМИН возможен с использованием электронных устройств перехвата информации, подключенных к каналам связи или техническим средствам обработки ПДн («аппаратные закладки»).

5.3. Угрозы несанкционированного доступа к информации, обрабатываемой в ИСПДн Комиссии.

В ИСПДн Комиссии угрозы НСД с применением программных и аппаратно-программных средств, которые реализуются при осуществлении несанкционированного, в том числе случайного доступа, в результате которого осуществляется нарушение конфиденциальности (копирования, несанкционированного распространения, несанкционированного ознакомления), целостности (уничтожения, изменения), достоверности и доступности (блокирования) ПДн, включают в себя:

угрозы доступа (проникновения) в операционную среду сервера с использованием штатного программного обеспечения (средств операционной системы или прикладных программ);

угрозы создания нештатных режимов работы программных (программно-аппаратных) средств за счет преднамеренных изменений служебных данных, игнорирования предусмотренных в штатных условиях ограничений на состав и характеристики обрабатываемой информации, искажения (модификации) самих данных и т.п.;

угрозы внедрения вредоносных программ (программ математического воздействия);

угрозы НСД, возникающие за счет непреднамеренных действий обслуживающего персонала системы.

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

Угрозы доступа (проникновения) в операционную среду ИСПДн Комиссии с использованием штатного программного обеспечения разделяются на угрозы непосредственного и удаленного доступа. Угрозы непосредственного доступа осуществляются с использованием программных и аппаратно-программных средств ввода/вывода компьютера. Угрозы удаленного доступа реализуются с использованием протоколов сетевого взаимодействия.

Угрозы внедрения вредоносных программ (программно-математического воздействия) нецелесообразно описывать с той же

детальностью, что и вышеуказанные угрозы, так как количество вредоносных программ уже значительно превышает сотни тысяч. Для осуществления защиты информации достаточно знать класс вредоносной программы, способы и последствия от ее внедрения (инфицирования).

5.4. Общая характеристика уязвимостей ИСПДн Комиссии.

Уязвимость ИСПДн Комиссии – недостаток или слабое место в системном, прикладном, программном и/или аппаратно-программном обеспечении системы, которое может быть использовано для реализации угрозы безопасности персональных данных.

Причиной возникновения уязвимостей являются:

ошибки при проектировании и разработке программного и/или аппаратно-программного обеспечения;

преднамеренные действия по внесению уязвимостей в ходе проектирования и разработки программного и/или аппаратно-программного обеспечения;

неправильные настройки программного и/или аппаратно-программного обеспечения, неправомерное изменение режимов работы устройств и программ;

несанкционированное внедрение и использование неучтенных программ с последующим необоснованным расходованием ресурсов (загрузка процессора, захват оперативной памяти и т.д.);

сбои в работе аппаратного и программного обеспечения (вызванные сбоями в электропитании, выходом из строя аппаратных элементов в результате старения и снижения надежности, внешними воздействиями электромагнитных полей технических устройств, внесение изменений в документацию и др.).

Различают следующие группы основных уязвимостей:

уязвимости системного программного обеспечения (в том числе протоколов сетевого взаимодействия);

уязвимости прикладного программного обеспечения (в том числе средств защиты информации).

5.4.1 Уязвимости системного программного обеспечения.

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

в микропрограммах, в прошивках запоминающих устройств;

в средствах ОС, предназначенных для управления локальными ресурсами ИСПДн Комиссии (обеспечивающих выполнение функций управления процессами, памятью, устройствами ввода/вывода, интерфейсом с пользователем и т.п.), драйверах, утилитах;

в средствах ОС, предназначенных для выполнения вспомогательных функций – утилитах (архивирования, дефрагментации и др.), системных обрабатывающих программах (компиляторах, компоновщиках, отладчиков и

т.п.), программах представления пользователю дополнительных услуг (специальных вариантах интерфейса, калькуляторах, играх и т.п.), библиотеках процедур различного назначения (библиотеках математических функций, функций ввода/вывода и т.п.);

в средствах коммуникационного взаимодействия (сетевых средствах) операционной системы.

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

функции, процедуры, изменение параметров которых определенным образом позволяет использовать их для несанкционированного доступа без обнаружения таких изменений операционной системой;

фрагменты кода программ («дыры», «закладки»), введенные разработчиком, позволяющие обходить процедуры идентификации, аутентификации, проверки целостности и др.;

отсутствие необходимых средств защиты (аутентификации, проверки целостности, проверки форматов сообщений, блокирования несанкционированно модифицированных функций и т.п.);

ошибки в программах (в объявлении переменных, функций и процедур, в кодах программ), которые при определенных условиях (например, при выполнении логических переходов) приводят к сбоям, в том числе к сбоям функционирования средств и систем защиты информации.

5.4.2. Уязвимости прикладного программного обеспечения.

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

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

Уязвимости прикладного программного обеспечения могут представлять собой:

функции и процедуры, относящие к разным прикладным программам и несовместимые между собой (не функционирующие в одной операционной среде) из-за конфликтов, связанных с распределением ресурсов системы;

функции, процедуры, изменение определенным образом параметров которых позволяет использовать их для проникновения в операционную среду ИСПДн Организации, а также использования штатных функций ОС, выполнения несанкционированного доступа без обнаружения таких изменений ОС;

фрагменты кода программ («дыры», «закладки»), введенные разработчиком, позволяющие обходить процедуры идентификации, аутентификации, проверки целостности и др., предусмотренные в ОС;

отсутствие необходимых средств защиты (аутентификации, проверка целостности, проверка форматов сообщений, блокирование несанкционированно модифицированных функций и т.п.);

ошибки в программах (в объявлении переменных, функций и процедур, кодах программ), которые при определенных условиях (например, при выполнении логических переходов) приводят к сбоям, в том числе к сбоям функционирования средств и систем защиты информации, к возможности несанкционированного доступа к информации.

5.5. Общая характеристика угроз непосредственного доступа в операционную среду ИСПДн Комиссии.

Для ИСПДн Комиссии можно рассматривать следующие угрозы непосредственного доступа в операционную среду:

угрозы, реализуемые в ходе загрузки ОС, направлены на перехват паролей или идентификаторов, модификацию ПО базовой системы ввода/вывода (BIOS), перехват управления загрузкой с изменением необходимой технологической информации получения НСД в операционную среду ИСПДн Комиссии. Чаще всего такие угрозы реализуются с использованием отчуждаемых носителей информации;

угрозы, реализуемые после загрузки операционной системы, направлены на выполнение несанкционированного доступа к информации с применением стандартных функций (уничтожение, копирование, перемещение, форматирование носителей информации и т.п.) операционной системы или какой-либо прикладной программы, а также с применением специально созданных для выполнения НСД программ (программ просмотра и модификации реестра, поиска текста в текстовых файлах и т.п.);

угрозы внедрения вредоносных программ. Реализация данных угроз определяется тем, какая из прикладных программ запускается пользователем или фактом запуска любой из прикладных программ.

5.6. Определение уровня исходной защищенности.

Определение уровня исходной защищенности производилось в соответствии с Методикой оценки угроз безопасности информации, утвержденной ФСТЭК России 05.02.2021 г.

Таблица 4. Показатели исходной защищенности ИСПДн.

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

Уровень исходной защищенности данных ИСПДн может быть оценен как «средний», исходя из того, что более 70% характеристик соответствуют уровню «средний» или выше.

При составлении перечня актуальных угроз безопасности ПДн полученной оценке степени исходной защищенности ставится в соответствие числовой коэффициент: Y1 = 5.

5.7. Определение вероятности реализации угроз в ИСПДн Комиссии.

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

Числовой показатель (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).

5.8. Определение вероятности реализации угроз в ИСПДн Комиссии и перечня актуальных угроз безопасности.

Таблица 5.

Наименование угрозы	Коэф. опред. Вероятность наступления угрозы (Y2)	Коэффициент реализуемости угрозы (Y=(Y1+Y2)/20)	Возможность реализации угрозы	Опасность угрозы (К3)	Актуальность угрозы
Угрозы утечки по техническим каналам передачи/обработки данных					
По видовым каналам					
Просмотр информации на дисплее сотрудниками, не допущенными к обработке персональных данных	2	0,35	Средняя	Низкая	Неактуально
Просмотр информации на дисплее посторонними лицами, находящимися в помещении, в котором ведется обработка персональных данных	2	0,35	Низкая	Средняя	Неактуально
Просмотр информации на дисплее посторонними лицами, находящимися за пределами помещения в котором, ведется обработка персональных данных	0	0,25	Низкая	Низкая	Неактуально

Наименование угрозы	Коэф. опред. Вероятность наступления угрозы (Y2)	Коэффициент реализуемости угрозы (Y=(Y1+Y2)/20)	Возможность реализации угрозы	Опасность угрозы (К3)	Актуальность угрозы
Просмотр информации с помощью специальных электронных устройств внедренных в помещении, в котором ведется обработка персональных данных	0	0,25	Низкая	Низкая	Неактуально
Угрозы НСД по программно-аппаратному каналу					
Угроза использования механизмов авторизации для повышения привилегий	2	0,35	Высокая	Средняя	Актуально
Угрозы несанкционированного доступа к BIOS	2	0,35	Высокая	Средняя	Актуально
Угрозы, реализуемые после загрузки ОС, направленные на уничтожение, копирование, перемещение, искажение данных	5	0,5	Высокая	Средняя	Актуально
Угрозы модификации настроек	5	0,5	Высокая	Средняя	Актуально
Угрозы внедрения вредоносного ПО	5	0,5	Высокая	Средняя	Актуально
Угроза возможности осуществления нарушителем деструктивного воздействия на систему путем эксплуатации уязвимостей программного обеспечения	5	0,5	Высокая	Средняя	Актуально
Угрозы фишинга	2	0,35	Высокая	Средняя	Актуально
Угроза доступа к защищаемым файлам с использованием обходного пути	2	0,35	Высокая	Средняя	Актуально
Угроза использования информации идентификации/аутентификации, заданной по умолчанию	2	0,35	Высокий	Средняя	Актуально
«Отказ в обслуживании»	5	0,5	Высокая	Средняя	Актуально
Угроза несанкционированного воздействия на средство защиты информации	2	0,35	Высокая	Средняя	Актуально
Угроза некорректного использования прозрачного прокси-сервера за счёт плагинов браузера	2	0,35	Высокая	Низкая	Не актуально
Угроза доступа/перехвата/изменения HTTP cookies	2	0,35	Высокая	Низкая	Не актуально
Угроза эксплуатации цифровой подписи программного кода	2	0,35	Высокая	Средняя	Не актуально
Несанкционированное отключение средств защиты	5	0,5	Высокая	Средняя	Неактуально
Угроза исследования механизмов работы программ	0	0,25	Низкая	Низкая	Неактуально
Угроза неправомерных действий в каналах связи	2	0,35	Высокая	Средняя	Не актуально

Наименование угрозы	Коэф. опред. Вероятность наступления угрозы (Y2)	Коэффициент реализуемости угрозы (Y=(Y1+Y2)/20)	Возможность реализации угрозы	Опасность угрозы (К3)	Актуальность угрозы
Угрозы хищения, несанкционированной модификации или блокирования информации за счет НСД с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий)					
Компьютерные вирусы	2	0,35	Высокая	Средняя	Актуально
Недекларированные возможности системного ПО и ПО для обработки персональных данных	0	0,25	Низкая	Низкая	Неактуально
Установка ПО, не связанного с исполнением служебных обязанностей	2	0,35	Средняя	Средняя	Актуально
Наличие аппаратных закладок в приобретаемых ПЭВМ	0	0,25	Низкая	Средняя	Неактуально
Внедрение аппаратных закладок посторонними лицами после начала эксплуатации ИСПДн	2	0,35	Низкая	Средняя	Актуально
Внедрение аппаратных закладок сотрудниками организации	2	0,35	Низкая	Средняя	Актуально
Внедрение аппаратных закладок обслуживающим персоналом (ремонтными организациями)	2	0,35	Низкая	Средняя	Актуально
Угрозы непреднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПДн в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молнии, пожаров, наводнений и т.п.) характера					
Угроза утраты носителей информации	5	0,5	Высокая	Средняя	Актуально
Непреднамеренная модификация (уничтожение) информации сотрудниками	5	0,5	Высокий	Средняя	Актуально
Непреднамеренное отключение средств защиты	2	0,35	Средняя	Средняя	Актуально
Выход из строя аппаратно-программных средств	2	0,35	Высокая	Средняя	Актуально
Сбой системы электроснабжения	0	0,25	Низкая	Низкая	Неактуально
Стихийное бедствие	0	0,25	Средняя	Низкая	Неактуально
Угрозы преднамеренных действий внутренних нарушителей					
Доступ к информации, модификация, уничтожение лицами, не допущенными к ее обработке	2	0,35	Низкая	Средняя	Неактуально
Угроза несанкционированного копирования защищаемой информации	2	0.35	Высокая	Средняя	Актуально
Разглашение информации, модификация, уничтожение сотрудниками, допущенными к ее обработке	5	0,5	Высокая	Средняя	Актуально
Угроза неподтверждённого ввода данных оператором в систему, связанную с безопасностью	0	0,25	Высокая	Средняя	Актуально

Наименование угрозы	Коэф. опред. Вероятность наступления угрозы (Y2)	Коэффициент реализуемости угрозы (Y=(Y1+Y2)/20)	Возможность реализации угрозы	Опасность угрозы (К3)	Актуальность угрозы
Угроза неправомерного ознакомления с защищаемой информацией	5	0,5	Высокая	Средняя	Актуально
Утечка атрибутов доступа	2	0,35	Высокий	Высокий	Актуально
Перехват за переделами контролируемой зоны	2	0,35	Высокий	Высокий	Актуально
Перехват в пределах контролируемой зоны внешними нарушителями	0	0,25	Низкая	Средняя	Неактуально
Перехват в пределах контролируемой зоны внутренними нарушителями	5	0,5	Высокая	Средняя	Актуально

Актуальными угрозами безопасности ИСПДн Организации являются:

угроза использования механизмов авторизации для повышения привилегий;

угрозы несанкционированного доступа к BIOS;

угрозы, реализуемые после загрузки ОС, направленные на уничтожение, копирование, перемещение, искажение данных;

угрозы модификации настроек;

угрозы внедрения вредоносного ПО;

угроза возможности осуществления нарушителем деструктивного воздействия на систему путем эксплуатации уязвимостей программного обеспечения;

угрозы фишинга;

угроза доступа к защищаемым файлам с использованием обходного пути;

угроза использования информации идентификации/аутентификации, заданной по умолчанию;

атака «Отказ в обслуживании»;

угроза несанкционированного воздействия на средство защиты информации;

компьютерные вирусы;

установка ПО, не связанного с исполнением служебных обязанностей;

внедрение аппаратных закладок посторонними лицами после начала эксплуатации ИСПДн;

внедрение аппаратных закладок сотрудниками организации;

внедрение аппаратных закладок обслуживающим персоналом (ремонтными организациями);

угроза утраты носителей информации;

непреднамеренная модификация (уничтожение) информации сотрудниками;

непреднамеренное отключение средств защиты;

выход из строя аппаратно-программных средств;

угроза несанкционированного копирования защищаемой информации;

разглашение информации, модификация, уничтожение сотрудниками, допущенными к ее обработке;

угроза неподтверждённого ввода данных оператором в систему, связанную с безопасностью;

угроза неправомерного ознакомления с защищаемой информацией;

утечка атрибутов доступа;

перехват за переделами контролируемой зоны;

перехват в пределах контролируемой зоны внутренними нарушителями.

6. Модель нарушителя ИСПДн.

6.1. Для всех ИСПДн Комиссии характерна одинаковая модель нарушителя.

На основании назначения ИСПДн Комиссии к нарушителям информационной безопасности ИСПДн Комиссии следует отнести субъекты следующих категорий:

неустановленные внешние субъекты (физические лица);

бывшие работники (пользователи);

лица, обеспечивающие функционирование информационных систем или обслуживающих инфраструктуру оператора (администрация, охрана, уборщики и т.п.);

пользователи информационной системы;

лица, привлекаемые для установки, наладки, монтажа, пуско-наладочных и иных работ;

администраторы информационной системы и администраторы безопасности.

Упомянутые выше потенциальные нарушители информационной безопасности ИСПДн, в большинстве своем не способны самостоятельно проводить лабораторные исследования криптосредств и/или средств обеспечивающих их функционирование, а также иметь отношения к научно-исследовательским организациям, которые могут самостоятельно осуществлять анализ средств СКЗИ и программно-технической среды их функционирования, а также разработку способов атак на них. В связи с этим, подобные исследовательские организации могут являться нарушителями информационной безопасности ИСПДн Организации исключительно в случае их привлечения к этому со стороны нарушителей, перечисленных выше типов путем организации сговора. При этом, поскольку такие научно-исследовательские организации, как правило, не могут рассматриваться как участники рынка, характерного для Комиссии, подобный сговор должен рассматриваться как совершаемый ими из корыстных побуждений. Вместе с тем, если учесть характер данных, которые обрабатываются, хранятся и передаются между объектами ИСПДн Комиссии, наличие такого рода сговора между нарушителями информационной безопасности систем Комиссии и специализированными исследовательскими организациями представляется маловероятным. По той же причине представляется невозможным привлечение этих организаций для реализации атак на ИСПДн Комиссии

физическими лицами (бывшими или действующими сотрудниками Комиссии).

Модель нарушителя информационной безопасности ИСПДн Комиссии строится исходя из конкретных категорий субъектов, их квалификации и мотивации действий с учетом используемых технологий обработки информации. Перечень видов и категорий нарушителей безопасности ПДн, обрабатываемых в ИСПДн Комиссии приведен в Таблице 6.

Таблица 6.

Вид нарушителя	Категория нарушителя	
	Категория I	Категория II
Внешние	Внешний нарушитель, не имеющий прав доступа в контролируемую зону	
Внутренние		1. Зарегистрированные пользователи ИСПДн Организации (пользователи, администраторы); 2. Незарегистрированные пользователи ИСПДн, но имеющие право доступа в контролируемую зону

При построении модели нарушителя принимаются следующие ограничения и предположения о характере действий нарушителей:

несанкционированный доступ может быть следствием как случайных, так и преднамеренных действий;

нарушитель, планируя атаки, скрывает свои несанкционированные действия от лиц, контролирующих соблюдение мер безопасности;

проведение работ по созданию способов и средств атак в научно-исследовательских центрах, специализирующихся в области разработки и анализа криптосредств и среды функционирования криптосредств (далее – СФК), не является целесообразным для нарушителей с учетом характера данных, обрабатываемых в ИСПДн Комиссии.

6.2. Внешние нарушители.

Внешний нарушитель не имеет права свободного доступа к системам и ресурсам ИСПДн Комиссии, находящимся в пределах контролируемой зоны, и может осуществлять атаки только с территории, расположенной вне контролируемой зоны, через выходящие за пределы контролируемой зоны каналы связи, а также технические каналы утечки информации.

К данному виду нарушителей относится внешний нарушитель, не имеющий прав доступа в контролируемую зону.

6.2.1. Внешние нарушители, не имеющие прав доступа в контролируемую зону.

6.2.1.1. Описание нарушителей.

Внешние нарушители данного вида характеризуются тем, что, как правило, не имеют возможности прямого доступа к элементам ИСПДн Комиссии, но при этом не исключается возможность доступа к коммуникационным линиям и оборудованию ИСПДн Комиссии, расположенным вне контролируемой зоны. Среди данного вида нарушителей можно выделить:

неустановленных внешних субъектов;

уволенных сотрудников Комиссии или уволенных сотрудников организаций, обеспечивающих техническое обслуживание и эксплуатацию ИСПДн Комиссии;

6.2.1.2. Предположения об имеющейся у нарушителя информации об объектах атак.

Уволенные сотрудники для реализации атак могут использовать свои знания о структуре сети, организации работы, защитных мерах и правах доступа и т.п.

Внешний нарушитель данного типа может иметь доступ к любому объему данных, распространяемому согласно установленному порядку и с помощью штатных средств системы по внешним каналам связи вне охраняемой зоны. Также он может располагать определенными фрагментами информации о топологии сети, об используемых коммуникационных протоколах и их сервисах, об особенностях используемого оборудования, системного, прикладного ПО и т.д. в объемах, доступных в свободной продаже.

Внешний нарушитель не должен (но гипотетически может) располагать именами зарегистрированных пользователей ИСПДн Комиссии, может вести разведку имен и паролей зарегистрированных пользователей.

6.2.1.3. Предположения об имеющихся у нарушителя средствах атаки.

Предполагается, что внешний нарушитель данного вида для реализации своих целей может обладать доступными в свободной продаже следующими техническими средствами и программным обеспечением:

средствами вычислительной техники (аппаратными и программными) общего назначения;

техническими и программными средствами, аналогичным средствам ИСПДн Комиссии, включая соответствующие средства каналообразования, маршрутизации и т.д.;

техническими и программными средствами защиты информации, включая СКЗИ, аналогичные используемым в ИСПДн Комиссии;

специализированными техническими и программными средствами, предназначенными для перехвата информации в общедоступных каналах связи.

6.2.1.4. Описание каналов атак.

Нарушители данного вида могут осуществлять атаки только из-за пределов контролируемой зоны через выходящие за пределы контролируемой зоны каналы связи, в том числе с использованием иных технических каналов утечки информации:

- проводить перехват и последующий анализ данных, циркулирующих по общедоступным каналам связи между отдельными элементами ИСПДн Комиссии;

- проводить попытки уничтожения, модификации и блокирования информации, передаваемой, обрабатываемой и хранимой в ИСПДн Комиссии;

- проводить попытки навязывания ложной информации;

- проводить атаки с целью вызвать отказы в работе отдельных компонентов ИСПДн Комиссии.

Доступным источником конфиденциальной информации для данного вида нарушителей могут быть отчуждаемые носители информации, выведенные установленным порядком из употребления. Нарушители данного вида не могут использовать для реализации атак штатные средства ИСПДн Комиссии.

6.3. Внутренние нарушители.

К внутренним нарушителям относятся лица, имеющие право постоянного или разового доступа к техническим средствам и информационным ресурсам ИСПДн Комиссии:

зарегистрированные пользователи ИСПДн;

лица, обеспечивающие функционирование информационных систем или обслуживающих инфраструктуру оператора (администратора, охрана, уборщики и т.д.)

лица, привлекаемые для установки, наладки, монтажа и пуско-наладочных работ;

администраторы информационных систем и администраторы безопасности.

В связи с этим принимаются следующие ограничения и предположения о характере действий потенциальных внутренних нарушителей:

работа по подбору кадров и специально проводимые организационно-технические мероприятия исключают возможность создания коалиций нарушителей, то есть объединения (заговоров) и направленных действий по преодолению подсистемы защиты двух и более нарушителей;

несанкционированные действия нарушителей могут не иметь преднамеренного характера и быть следствием ошибок пользователей, администраторов, эксплуатирующего и обслуживающего персонала;

легальный доступ посторонних лиц в помещения, где размещены компоненты ИСПДн Комиссии, и к информационным ресурсам ИСПДн исключается принятыми организационными и/или техническими мерами по обеспечению порядка доступа в помещения, охране территории и организации пропускного режима на объектах, а также внедрением необходимых защитных мер и устройств в оборудование ИСПДн;

По возможным сценариям воздействия внутренние нарушители могут быть классифицированы как злоумышленники, то есть лица, которые целенаправленно стараются преодолеть систему защиты и нанести ущерб, и нарушители, которые совершают несанкционированные действия неумышленно, но эти действия также могут нанести ущерб и должны учитываться при построении системы защиты.

Возможности внутреннего нарушителя существенно зависят от действующих в пределах контролируемой зоны ограничительных факторов, реализации комплекса административных, режимных и организационно-технических мер, направленных на предотвращение и пресечение несанкционированных действий пользователей и администраторов системы, нарушения порядка допуска и контроля сторонних лиц внутри контролируемой зоны, предотвращение несанкционированного доступа пользователей к ресурсам ИСПДн Комиссии, а так же контроль за порядком обращения конфиденциальной информации.

6.3.1. Сотрудник Организации, не являющийся зарегистрированным пользователем ИСПДн Организации, но имеющий право доступа в контролируемую зону.

6.3.1.1. Описание нарушителей (субъектов атак).

Внутренние нарушители характеризуются тем, что имеют практически неограниченную возможность по доступу к элементам ИСПДн и их коммуникационным линиям. К внутренним нарушителям данного вида относятся технический и вспомогательный персонал подразделений жизнеобеспечения объектов Комиссии, имеющий доступ в помещения, где установлено оборудование ИСПДн Комиссии.

6.3.1.2. Предположения об имеющейся у нарушителя информации об объектах атак.

Предполагается, что нарушители данного типа дополнительно к информации, имеющейся у внешнего нарушителя и описанной в п. 6.2.1.2, могут:

располагать именами (логинами) зарегистрированных пользователей ИСПДн, а также вести разведку паролей зарегистрированных пользователей;

иметь представление об организации работы пользователей, порядке и правилах создания, хранения и передачи информации.

6.3.1.3. Предположения об имеющихся у нарушителях средствах атак.

Предполагается, что внешний нарушитель данного вида дополнительно к средствам осуществления атак, описанных выше в пункт 6.2.1.3, может использовать серийно изготовляемое специальное оборудование и свободно распространяемое ПО, предназначенные для сканирования и копирования информационных ресурсов рабочих станций, изменения конфигураций рабочих станций, включая конфигурации средств защиты информации и/или внесения в систему вредоносного программного кода.

6.3.1.4. Описание каналов атак.

Дополнительно к атакам, доступным нарушителю, описанному в п. 6.2.1.4, рассматриваемый тип нарушителя может осуществлять попытки несанкционированного доступа к ресурсам ИСПДн Комиссии с целью

получения информации, ее подмены или уничтожения, включая обход существующих средств защиты информации, с использованием следующих атак:

подбора и подмены идентификатора (выдача себя за зарегистрированного пользователя);

получения аутентификационной информации легальных пользователей посредством сканирования открытых портов на рабочих станциях и серверах;

атак, основанных на переполнении буфера, генерируемых с использованием специализированных программных средств;

внедрения вредоносного ПО;

попыток временной или полной остановки работы посредством атак класса «отказ в обслуживании».

Доступным источником конфиденциальной информации для данного вида нарушителей могут быть отчуждаемые носители информации, выведенные установленным порядком из употребления.

6.3.2. Зарегистрированные пользователи ИСПДн Комиссии.

Зарегистрированный пользователь ИСПДн Комиссии имеет санкционированный доступ к работе в системе с использованием штатных аппаратных и программных средств.

В свою очередь, зарегистрированный пользователь может быть допущен к использованию шифровальных (криптографических) средств, не имея легального доступа к СКЗИ и их ключевой информации.

6.3.2.1. Описание нарушителей (субъектов атак).

Зарегистрированный пользователь, имеющий статус администратора и отвечающий за обеспечение безопасности, обладает полной информацией о системе (сети), имеет доступ ко всем техническим средствам обработки информации и данным, к средствам защиты информации и протоколирования, в том числе и к средствам криптозащиты, обладает правами конфигурирования и административной настройки. Единственным исключением для таких пользователей может являться отсутствие доступа ко всему объекту ключевой информации, используемой в системе. Зарегистрированные пользователи такой категории относятся к числу привилегированных пользователей, назначаемых из числа особо доверенных лиц. Реализация необходимых организационно-технических мер, обеспечивающих выполнение требований по безопасности при приеме на работу данной категории сотрудников, а также контроль за выполнением ими своих должностных обязанностей и соблюдением установленных правил и инструкций позволяет не рассматривать их в качестве потенциальных нарушителей.

Предполагается также, что пользователи, осуществляющие удаленный доступ к защищаемым ресурсам, по своим возможностям не превосходят возможностей локальных пользователей, имеющих доступ к штатным средствам системы, и поэтому они отдельно не рассматриваются.

6.3.2.2. Предположения об имеющейся у нарушителя информации об объектах атак.

Предполагается, что зарегистрированный пользователь знает, по меньшей мере, одно легальное имя доступа.

Кроме того, зарегистрированный пользователь может располагать всей информацией о топологии и технических средствах обработки информации сети, полным объемом конфиденциальных данных, к которым данный пользователь имеет доступ, и любыми фрагментами неконфиденциальных (не защищаемых от доступа данного пользователя) данных, обладать всеми необходимыми атрибутами, обеспечивающими доступ (паролем), имеет описание используемых в СКЗИ криптографических алгоритмов и протоколов, а также ключевую информацию к шифровальным средствам в объеме, доступном одному пользователю.

Зарегистрированный пользователь знает специфику задач, решаемых в ИСПДн Комиссии, и функциональные особенности работы системы, а также хранения, обработки и передачи информации.

6.3.2.3. Предположения об имеющихся у нарушителя средствах атак.

Нарушители данного вида обладают возможностями использования доступных в свободной продаже технических и программных средств для:

внесения ошибок и программных закладок в системное и прикладное ПО;

внедрения вредоносных программ;

хищения, уничтожения, модификации, блокирования информации и навязывания ложной информации.

6.3.2.4. Описание каналов атак.

Зарегистрированный пользователь дополнительно имеет возможность прямого физического и прямого (не межсетевого) доступа к некоторому подмножеству ресурсов сети. Прямой доступ к ресурсам может быть использован для атак на технические средства обработки информации.

Нарушители данного вида для реализации атак могут использовать каналы связи, расположенные как внутри, так и вне контролируемой зоны.

6.4. Определение типов нарушителей.

При определении типа нарушителя в рамках данного документа оцениваются:

степень информированности нарушителя;

возможность нарушителя по использованию средств атаки.

При определении ограничений на степень информированности нарушителя рассматривались следующие сведения:

содержание технической документации на технические и программные компоненты СФК;

все возможные данные, передаваемые в открытом виде по каналам связи, не защищенным от НСД к информации организационно-техническими мерами;

сведения о линиях связи, по которым передается защищаемая информация;

все проявляющиеся в каналах связи, не защищенных от НСД к информации организационно-техническими мерами, нарушения правил эксплуатации криптосредства и СФК;

все проявляющиеся в каналах связи, не защищенных от НСД к информации организационно-техническими мерами, неисправности и сбои технических криптосредств и СФК;

сведения, получаемые в результате анализа любых сигналов от технических криптосредств и СФК, которые может перехватить нарушитель.

Таблица 7.

Соответствие типа нарушителя и степени его информативности.

Тип нарушителей	Степень информированности
Н1 – Н2	Располагают только доступными в свободной продаже аппаратными компонентами криптосредства и СФК
Н3 – Н6	Могут располагать информацией обо всех сетях связи, работающих на едином ключе
Н5 – Н6	Располагают наряду с доступной в свободной продаже документацией на криптосредство и СФК исходными текстами прикладного программного обеспечения
Н6	Располагает всей документацией на криптосредство и СФК

При определении ограничений на имеющиеся у нарушителя средства атак, в частности, рассматриваются:

аппаратные компоненты криптосредства и СФК;

доступные в свободной продаже технические средства и программное обеспечение;

специально разработанные технические средства и программное обеспечение;

штатные средства.

Таблица 8.

Возможности нарушителей по использованию средств атак.

<table>
<tr><th>Тип нарушителя</th><th>Аппаратные компоненты криптосредства и СФК</th><th>Штатные средства</th><th>Лабораторные исследования</th></tr>
<tr><td>Н1</td><td rowspan="2">Располагают только доступными в свободной продаже аппаратными компонентами криптосредства и СФК</td><td>Могут использовать штатные средства только в том случае, если они расположены за пределами контролируемой зоны</td><td rowspan="3">–</td></tr>
<tr><td>Н2</td><td rowspan="4">Возможности по использованию штатных средств зависят от реализованных в информационной системе организационных мер</td></tr>
<tr><td>Н3</td><td rowspan="3">Дополнительные возможности по получению аппаратных компонент криптосредства и СФК зависят от реализованных в информационной системе организационных мер</td></tr>
<tr><td>Н4</td><td rowspan="2">Могут проводить лабораторные исследования криптосредств, используемых за пределами контролируемой зоны</td></tr>
<tr><td>Н5</td></tr>
</table>

Н6	Располагают любыми аппаратными компонентами криптосредства и СФК		информационной системы

В соответствии с классификацией ФСБ России и с учетом сформулированных предположений об имеющихся у нарушителей возможностях нарушители ИСПДн Комиссии подразделяются на следующие категории и типы, которые представлены в Таблице 9.

Таблица 9.

Виды нарушителей безопасности персональных данных

Вид нарушителя	Категория		Тип нарушителя
	Категория I	Категория II	
Внешние	Внешний нарушитель, не имеющий прав доступа в контролируемую зону		Н1
Внутренние		1. Зарегистрированные пользователи ИСПДн Организации (пользователи)	Н2
		2. Незарегистрированные пользователи ИСПДн, но имеющие право доступа в Контролируемую зону	Н3

При этом возможности нарушителя типа Нi+1 включают в себя возможности нарушителя Нi (1< i <5), а следовательно, при выборе необходимого уровня криптографической защиты ПДн следует рассматривать наивысший тип.

Таблица 8.

Классификация ИСПДн Организации по уровням защиты от НСД к ПДн

ИСПДн Комиссии	Тип нарушителя	Уровни защиты от НСД к ПДн
Все	Н3	АК3

6.5. Уровень криптографической защиты.

Возможности внешнего и внутреннего нарушителя безопасности ПДн при их обработке в ИСПДн Комиссии соответствуют возможностям нарушителя типа Н1, Н2 и Н3 – соответственно, согласно классификации нарушителей, приведенной в Приказе ФСБ России № 378 10.07.2014 г «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 уровня защищенности», и «Методических рекомендациях по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных система персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности» утвержденные руководством 8 Центра ФСБ России №

149/7/2/6-432 от 31 марта 2015 г., криптографические средства защиты информации, используемые для защиты ПДн, обрабатываемых в ИСПДн Комиссии, должны обеспечивать криптографическую защиту по уровню не ниже уровня КС3.

7. Выводы.

7.1. Атаки внешнего нарушителя, направленные на каналы связи, посредством перехвата информации и последующего ее анализа, уничтожения, модификации и блокирования информации с использованием, в том числе, уязвимостей программной среды, а также утечка информации по техническим каналам подлежат нейтрализации организационными и техническими мероприятиями.

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

7.3. Ввиду исключительной роли в ИСПДн Комиссии лиц типа Н3, в число этих лиц должны включаться только доверенные лица, к которым применен комплекс особых организационных мер по их подбору, принятию на работу, назначению на должность и контролю выполнения функциональных обязанностей.

7.4. Лица типа Н3 относятся к вероятным нарушителям. Среди лиц типа Н3 наиболее опасными вероятными нарушителями являются пользователи ИСПДн, уполномоченный персонал, который на договорной основе имеет право на техническое обслуживание и модификацию компонентов ИСПДн, а также администраторы информационной системы и администраторы безопасности.

На основании построенной модели нарушителя, в частности, описания возможностей нарушителей и Постановления Правительства № 1119 от 1 ноября 2012 г. можно сделать вывод, что для ИСПДн Комиссии актуальны угрозы 3-го типа, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в ИСПДн.

Представленная Модель угроз с описанием вероятного нарушителя для ИСПДн должна использоваться при формировании обоснованных требований безопасности информации и при проектировании СЗПДн ИСПДн. Средства защиты информации, используемые для защиты ПДн, обрабатываемых в ИСПДн Организации, должны иметь сертификаты соответствия по требованиям информационной безопасности соответствующего класса.