УТВЕРЖДАЮ

директор АО «Хабаровская горэлектросеть»

_____ А.Ю. Соколов

«____» _____ 2017 г.

Политика информационной безопасности информационных систем персональных данных АО «Хабаровская горэлектросеть»

г. Хабаровск 2017

Содержание

ОПРЕДЕЛЕНИЯ

В настоящем документе используются следующие термины и их определения.

Автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники.

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.

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

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

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

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

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

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

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

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

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

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

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

Нарушитель безопасности персональных данных – физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является

нарушение безопасности персональных данных при их обработке техническими средствами в информационных системах персональных данных.

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

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

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

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

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

Обработка персональных данных – любое действие (операции) 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, организующее и (или) осуществляющее обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

Технические средства информационной системы персональных данных – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки ПДн (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и

другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации, применяемые в информационных системах.

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

Персональные данные – любая информация, относящаяся прямо или косвенно к 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.

Предоставление персональных данных – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

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 невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.

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

Уязвимость – слабость в средствах защиты, которую можно использовать для нарушения системы или содержащейся в ней информации.

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

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 ИСПДн АО «Хабаровская горэлектросеть» (далее – Общество**)** является официальным документом.

Политика разработана в соответствии с целями, задачами и принципами обеспечения безопасности персональных данных изложенных в Концепции информационной безопасности ИСПДн Общества.

Политика разработана в соответствии с требованиями Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» и постановления Правительства Российской Федерации от 01.11.2012 N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», на основании:

- Приказ ФСТЭК России от 18.02.2013 № 21 (ред. от 23.03.2017) «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
- Приказ ФСБ от 10 июля 2014 года № 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».

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 Общества.

1 Общие положения

Целью настоящей Политики является обеспечение безопасности объектов защиты Общества 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 персональных данных представлен в Перечне персональных данных, подлежащих защите.

Состав ИСПДн Общества подлежащих защите:

- ИСПДн «ХГЭС»;
- ИСПДн «Дальсистема»;
- ИСПДн «Электросеть».

Область действия

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

2 Система защиты персональных данных

Система защиты персональных данных (СЗПДн), строится на основании:
- Заключения по результатам аудита информационных систем персональных данных;
- Перечня персональных данных, подлежащих защите;
- Акта классификации информационной системы персональных данных;
- Модели угроз безопасности персональных данных;
- Положения о разграничении прав доступа к обрабатываемым персональным данным;
- Руководящих документов ФСТЭК, ФСБ России, Роскомнадзора.

На основании этих документов определяется необходимый уровень защищенности ПДн ИСПДн Общества. На основании анализа актуальных угроз безопасности ПДн описанного в Модели угроз и Заключении по результатам аудита информационных систем персональных данных, делается заключение о необходимости использования технических средств и организационных мероприятий для обеспечения безопасности ПДн. Выбранные необходимые мероприятия отражаются в Плане мероприятий по обеспечению защиты ПДн.

Для ИСПДн должен быть составлен список используемых технических средств защиты, а так же программного обеспечения участвующего в обработке ПДн, на всех элементах ИСПДн: АРМ пользователей; сервера приложений; СУБД; граница 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:
- программные, программно-аппаратные комплексы защиты от НСД к информации;
- 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 должен включать:
- управление и разграничение доступа пользователей;
- регистрацию и учет действий с информацией;
- обеспечивать целостность данных;
- производить обнаружений вторжений.
- анализ защищенности;
- безопасное межсетевое взаимодействие

Перечень используемых средств должен поддерживаться в актуальном состоянии. При изменении состава технических средств защиты или элементов ИСПДн, соответствующие изменения должны быть внесены в Перечень и утверждены руководителем Общества.

3 Требования к подсистемам СЗПДн

3.1 Общие требования к СЗПДн

В СЗПДн должны использоваться только средства защиты информации, сертифицированные в установленном порядке на соответствие функциональным требованиям информационной безопасности, установленным порядком в системе сертификации ФСТЭК России или ФСБ России.

В соответствии с положением «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» (утвержденное приказом ФСТЭК России от 18.02.2013 № 21) применяемые в СЗПДн методы и способы защиты информации от НСД должны обеспечивать реализацию следующих функций:

- управления доступом;
- регистрации и учета;
- обеспечения целостности;
- анализа защищенности;
- обеспечения безопасного межсетевого взаимодействия;
- обнаружения вторжений;
- обеспечения антивирусной защиты;
- централизованного управления.

Реализация данных требований осуществляется в соответствующих подсистемах устанавливаемых технических средств защиты информации.

3.1.1 Требования к управлению доступом

Управление доступом должно обеспечивать идентификацию и проверку подлинности пользователя при входе в систему информационной системы по идентификатору (коду) и паролю условно-постоянного действия длиной не менее шести буквенно-цифровых символов.

3.1.2 Требования к регистрации и учету

Регистрация и учет:

- регистрация входа (выхода) пользователей в систему (из системы), либо регистрация загрузки и инициализации операционной системы и ее программного останова. Регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения информационной системы. В параметрах регистрации указываются дата и время входа (выхода) пользователя в систему (из системы) или загрузки (останова) системы, результат попытки входа (успешная или неуспешная), идентификатор (код или фамилия) пользователя, предъявленный при попытке доступа, код или пароль, предъявленный при неуспешной попытке;
- регистрация выдачи печатных (графических) документов на бумажный носитель. В параметрах регистрации указываются дата и время выдачи (обращения к подсистеме вывода), спецификация устройства выдачи (логическое имя (номер) внешнего устройства), краткое содержание

документа (наименование, вид, шифр, код), идентификатор пользователя, запросившего документ;
- регистрация запуска (завершения) программ и процессов (заданий, задач), предназначенных для обработки персональных данных. В параметрах регистрации указываются дата и время запуска, имя (идентификатор) программы (процесса, задания), идентификатор пользователя, запросившего программу (процесс, задание), результат запуска (успешный, неуспешный);
- регистрация попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам. В параметрах регистрации указываются дата и время попытки доступа к защищаемому файлу с указанием ее результата (успешная, неуспешная), идентификатор пользователя, спецификация защищаемого файла;
- регистрация попыток доступа программных средств к дополнительным защищаемым объектам доступа (терминалам, техническим средствам, узлам сети, линиям (каналам) связи, внешним устройствам, программам, томам, каталогам, файлам, записям, полям записей). В параметрах регистрации указываются дата и время попытки доступа к защищаемому объекту с указанием ее результата (успешная, неуспешная), идентификатор пользователя, спецификация защищаемого объекта (логическое имя (номер));
- учет всех защищаемых носителей информации с помощью их маркировки и занесение учетных данных в журнал учета с отметкой об их выдаче (приеме);
- очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти информационной системы и внешних накопителей;
- учет всех защищаемых носителей информации с помощью их маркировки и занесение учетных данных в журнал учета с отметкой об их выдаче (приеме).

3.1.3 Требования к обеспечению целостности

Функция обеспечения целостности:

- обеспечение целостности программных средств системы защиты персональных данных, обрабатываемой информации, а также неизменность программной среды. При этом целостность программных средств проверяется при загрузке системы по контрольным суммам компонентов средств защиты информации, а целостность программной среды обеспечивается использованием трансляторов с языков высокого уровня и отсутствием средств модификации объектного кода программ в процессе обработки и (или) хранения защищаемой информации
- физическая охрана информационной системы (устройств и носителей информации), предусматривающая контроль доступа в помещения информационной системы посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения информационной системы и хранилище носителей информации
- периодическое тестирование функций системы защиты персональных данных при изменении программной среды и пользователей информационной системы с помощью тест-программ, имитирующих попытки несанкционированного доступа

- наличие средств восстановления системы защиты персональных данных, предусматривающих ведение двух копий программных компонентов средств защиты информации, их периодическое обновление и контроль работоспособности

3.1.4 Требования к подсистеме криптографической защиты

Криптографическая защита должна обеспечивать:

- шифрование данных, содержащихся в областях оперативной памяти;
- вычисление имитовставки для данных, содержащихся в областях оперативной памяти;
- вычисление электронной цифровой подписи, содержащихся в областях оперативной памяти;
- вычисление значения хэш-функций, содержащихся в областях оперативной памяти;

3.1.5 Требования к безопасному межсетевому взаимодействию

Безопасное межсетевое взаимодействие должно обеспечивать:

- фильтрацию на сетевом уровне независимо для каждого сетевого пакета (решение о фильтрации принимается на основе сетевых адресов отправителя и получателя или на основе других эквивалентных атрибутов);
- фильтрацию пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств;
- фильтрацию с учетом входного и выходного сетевого интерфейса как средства проверки подлинности сетевых адресов;
- фильтрацию с учетом любых значимых полей сетевых пакетов;
- регистрацию и учет фильтруемых пакетов (в параметры регистрации включаются адрес, время и результат фильтрации);
- идентификацию и аутентификацию администратора межсетевого экрана при его локальных запросах на доступ по идентификатору (коду) и паролю условно-постоянного действия;
- регистрацию входа (выхода) администратора межсетевого экрана в систему (из системы) либо загрузки и инициализации системы и ее программного останова (регистрация выхода из системы не проводится в моменты аппаратурного отключения межсетевого экрана);
- регистрацию запуска программ и процессов (заданий, задач);
- контроль целостности своей программной и информационной части;
- восстановление свойств межсетевого экрана после сбоев и отказов оборудования;
- регламентное тестирование реализации правил фильтрации, процесса регистрации, процесса идентификации и аутентификации администратора межсетевого экрана, процесса регистрации действий администратора межсетевого экрана, процесса контроля за целостностью программной и информационной части, процедуры восстановления.

3.1.6 Требования к обнаружению вторжений

Функция обнаружения вторжений должна исключать нарушения или предпосылки к нарушению установленных требований по обеспечению безопасности персональных данных при взаимодействии информационной системы с сетью связи общего пользования.

3.1.7 Требования к анализу защищённости

Функция анализа защищённости должна обеспечивать выявление уязвимостей, связанных с ошибками в конфигурировании программного обеспечения информационной системы (определение топологии и ресурсов сети, поиск уязвимостей, поиск остаточной информации в памяти, локальный аудит паролей ОС, перехват и анализ сетевого трафика, аудит ПО и аппаратной конфигурации, аудит паролей к сетевым сервисам).

3.1.8 Требования к антивирусной защите

Антивирусная защита должна строиться на основе антивирусных средств, сертифицированных по требованиям ФСТЭК, ФСБ России и обеспечивать:

– проверку файлов, веб-страниц, почтовых сообщений;
– проактивную защиту от неизвестных угроз;
– защиту от хакерских атак;
– защиту от спама и фишинга в почтовых программах;
– самозащиту АВС от попыток выключения со стороны вредоносного ПО;
– регулярные и экстренные обновления;
– проверка определенных файлов (все файлы, логические диски, каталоги и т.д.);
– проверка оперативной памяти и всех файлов автозапуска;
– непрерывный, в течение всего времени работы, контроль вирусной ситуации;
– целостность передаваемой информации между компонентами антивирусных средств посредством механизма контрольных сумм;
– нейтрализацию (или удаление) программного кода компьютерного вируса в зараженных объектах;
– блокирование компьютерных вирусов;

3.1.9 Требования к централизованному управлению системой защиты ИСПДн

Централизованное управление должно осуществлять:

– мониторинг контролируемых рабочих станций в режиме реального времени;
– сбор и анализ данных, полученных от контролируемых рабочих станций.

4 Пользователи ИСПДн

В Концепции информационной безопасности определены основные категории пользователей. На основании этих категории должна быть произведена типизация пользователей ИСПДн, определен их уровень доступа и возможностей.

В ИСПДн Общества можно выделить следующие категории пользователей, участвующих в обработке и хранении ПДн: Программисты-разработчики; Администратор безопасности информации (далее – Администратор); Пользователи ИСПДн.

Данные о типах пользователях, уровне их доступа и информированности должны быть отражены в Положении о разграничении прав доступа к обрабатываемым персональным данным.

4.1 Администратор безопасности информации

Администратор, сотрудник Учреждения, 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 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;
- имеет доступ к средствам защиты информации и протоколирования и к части ключевых элементов ИСПДн.

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; устанавливать доверительные отношения своей защищенной сети с сетями других предприятий, учреждений и организаций.

4.2 Пользователь ИСПДн

Пользователь ИСПДн, сотрудник Учреждения, осуществляющий обработку ПДн. Обработка ПДн включает: возможность просмотра ПДн, ручной ввод ПДн в систему ИСПДн, формирование справок и отчетов по информации, полученной из ИСПД. Пользователь не имеет полномочий для управления подсистемами обработки данных и СЗПДн.

Пользователь 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.

5 Требования к персоналу по обеспечению защиты ПДн

Все сотрудники Общества, 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 непосредственный начальник подразделения, в которое он поступает, обязан организовать его ознакомление с должностной инструкцией и 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 Общества, 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 Общества должны следовать установленным процедурам поддержания режима безопасности ПДн при выборе и использовании паролей (если не используются технические средства аутентификации).

Сотрудники Общества 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 информационной системой Учреждения, третьим лицам.

При работе с ПДн в ИСПДн сотрудники Общества 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 Общества 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.

6 Должностные обязанности пользователей ИСПДн

Должностные обязанности пользователей ИСПДн описаны в следующих документах:

- Инструкция администратора безопасности информации;
- Инструкция пользователя ИСПДн;
- Инструкция пользователя при возникновении внештатных ситуаций.;
- Должностной регламент ответственного за организацию обработки и обеспечение безопасности персональных данных.

7 Ответственность сотрудников Общества

В соответствии со ст. 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 РФ 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 УК РФ).

Администратор безопасности информации несет ответственность за все действия, совершенные от имени его учетной записи или системных учетных записей, если не доказан факт несанкционированного использования учетных записей.

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

Приведенные выше требования нормативных документов по защите информации должны быть отражены в Положениях о подразделениях Учреждения, осуществляющих обработку ПДн в ИСПДн и должностных инструкциях сотрудников Учреждения.

Необходимо внести в Положения о подразделениях Общества, осуществляющих обработку ПДн в ИСПДн сведения об ответственности их руководителей и сотрудников за разглашение и несанкционированную модификацию (искажение, фальсификацию) ПДн, а также за неправомерное вмешательство в процессы их автоматизированной обработки.

8 Список использованных источников

Основными нормативно-правовыми и методическими документами, на которых базируется настоящее Положение являются:

- Федеральный Закон от 27.07.2006 г. № 152-ФЗ «О персональных данных»;
- «Положение об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», утвержденное Постановлением Правительства РФ от 01.11.2012 №1119;
- Приказ ФСТЭК России от 18.02.2013 № 21 (ред. от 23.03.2017) «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
- «Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», утвержденное Постановлением Правительства РФ от 15.09.2008 г. № 687;
- «Требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных», утвержденные Постановлением Правительства РФ от 06.07.2008 г. № 512;
- Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утв. Зам. директора ФСТЭК России 15.02.08 г. (ДСП);
- Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утв. Зам. директора ФСТЭК России 15.02.08 г. (ДСП).

Приложение № 1к Политике
информационной безопасности
информационных систем
персональных данных

МЕТОДЫ И СПОСОБЫ ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА В ЗАВИСИМОСТИ ОТ КЛАССА ИНФОРМАЦИОННОЙ СИСТЕМЫ

Классы / Требования	3кл/2кл	3кл/2кл	3кл/2кл	3кл	2кл	1кл	1кл	1кл	1кл
	Однопользовательская	Многопользовательская Равные права	Многопользовательская Разные права	Подд. к сетям Международного обмена	Подд. к сетям Международного обмена	Однопользовательская	Многопользовательская Равные права	Многопользовательская Разные права	Под к сетям МежОб
1	2	3	4	5	6	7	8	9	10
Управление доступом									
идентификация и проверка подлинности пользователя при входе в систему по **идентификатору (коду)** и **паролю** условно-постоянного действия длиной не менее шести буквенно-цифровых символов		+					+	+	
идентификация и проверка подлинности пользователя при входе в систему информационной системы **по паролю** условно-постоянного действия длиной не менее шести буквенно-цифровых символов	+		+			+			
идентификация технических средств информационных систем и каналов связи, внешних устройств информационных систем по их логическим адресам (номерам)							+		
идентификация программ, томов, каталогов, файлов, записей, полей записей по именам							+	+	

Классы / Требования	3кл/2кл	3кл/2кл	3кл/2кл	3кл	2кл	1кл	1кл	1кл	1кл
	Однопользовательская	Многопользовательская Равные права	Многопользовательская Разные права	Подд. к сетям Международного обмена	Подд. к сетям Международного обмена	Однопользовательская	Многопользовательская Равные права	Многопользовательская Разные права	Под к сетям МежОб
1	2	3	4	5	6	7	8	9	10
идентификация терминалов, технических средств, узлов сети, каналов связи, внешних устройств по логическим именам								+	
контроль доступа пользователей к защищаемым ресурсам в соответствии с матрицей доступа								+	
Регистрация и учет									
регистрация входа (выхода) пользователя в систему (из системы) либо регистрация загрузки и инициализации операционной системы и ее программного останова. Регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения информационной системы. В параметрах регистрации указываются дата и время входа (выхода) пользователя в систему (из системы) или загрузки (останова) системы;	+								
учет всех защищаемых носителей информации с помощью их маркировки и занесение учетных данных в журнал учета	+	+				+			
регистрация входа (выхода) пользователя в систему (из системы) либо регистрация загрузки и инициализации операционной системы и ее программного останова. Регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения информационной системы. В параметрах регистрации указываются дата и время входа (выхода) пользователя в систему (из системы) или загрузки (останова) системы, **результат попытки входа**		+				+			

Классы / Требования	3кл/2кл	3кл/2кл	3кл/2кл	3кл	2кл	1кл	1кл	1кл	1кл
	Однопользовательская	Многопользовательская Равные права	Многопользовательская Разные права	Подд. к сетям Международного обмена	Подд. к сетям Международного обмена	Однопользовательская	Многопользовательская Равные права	Многопользовательская Разные права	Под к сетям МежОб
1	2	3	4	5	6	7	8	9	10
(успешная или неуспешная)									
учет всех защищаемых носителей информации с помощью их маркировки и занесение учетных данных в журнал учета с отметкой об их выдаче (приеме)			+				+	+	
регистрация входа (выхода) пользователя в систему (из системы) либо регистрация загрузки и инициализации операционной системы и ее программного останова. Регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения информационной системы. В параметрах регистрации указываются дата и время входа (выхода) пользователя в систему (из системы) или загрузки (останова) системы, результат попытки входа (успешная или неуспешная)**, идентификатор (код или фамилия) пользователя, предъявленный при попытке доступа**			+				+		

Классы / Требования	3кл/2кл	3кл/2кл	3кл/2кл	3кл	2кл	1кл	1кл	1кл	1кл
	Однопользовательская	Многопользовательская Равные права	Многопользовательская Разные права	Подд. к сетям Международного обмена	Подд. к сетям Международного обмена	Однопользовательская	Многопользовательская Равные права	Многопользовательская Разные права	Под к сетям МежОб
1	2	3	4	5	6	7	8	9	10
регистрация входа (выхода) пользователей в систему (из системы), либо регистрация загрузки и инициализации операционной системы и ее программного останова. Регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения информационной системы. В параметрах регистрации указываются дата и время входа (выхода) пользователя в систему (из системы) или загрузки (останова) системы, результат попытки входа (успешная или неуспешная), идентификатор (код или фамилия) пользователя, предъявленный при попытке доступа, **код или пароль, предъявленный при неуспешной попытке**								+	
регистрация выдачи печатных (графических) документов на бумажный носитель. В параметрах регистрации указываются дата и время выдачи (обращения к подсистеме вывода), краткое содержание документа (наименование, вид, код), спецификация устройства выдачи (логическое имя (номер) внешнего устройства)						+			
регистрация выдачи печатных (графических) документов на бумажный носитель. В параметрах регистрации указываются дата и время выдачи (обращения к подсистеме вывода), спецификация устройства выдачи (логическое имя (номер) внешнего устройства), краткое содержание документа (наименование, вид, **шифр**, код), **идентификатор пользователя**, запросившего документ							+	+	

Классы / Требования	3кл/2кл	3кл/2кл	3кл/2кл	3кл	2кл	1кл	1кл	1кл	1кл
	Однопользовательская	Многопользовательская Равные права	Многопользовательская Разные права	Подд. к сетям Международного обмена	Подд. к сетям Международного обмена	Однопользовательская	Многопользовательская Равные права	Многопользовательская Разные права	Под к сетям МежОб
1	2	3	4	5	6	7	8	9	10
дублирующий учет защищаемых носителей информации						+	+		
очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти информационной системы и **внешних носителей** информации						+	+		
очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти информационной системы и **внешних накопителей**								+	
регистрация запуска (завершения) программ и процессов (заданий, задач), предназначенных для обработки персональных данных. В параметрах регистрации указываются дата и время запуска, имя (идентификатор) программы (процесса, задания), идентификатор пользователя, запросившего программу (процесс, задание), результат запуска (успешный, неуспешный)							+	+	
регистрация попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам. В параметрах регистрации указываются дата и время попытки доступа к защищаемому файлу с указанием ее результата (успешная, неуспешная), идентификатор пользователя, спецификация защищаемого файла							+	+	

Требования \ Классы	3кл/2кл	3кл/2кл	3кл/2кл	3кл	2кл	1кл	1кл	1кл	1кл
	Однопользовательская	Многопользовательская Равные права	Многопользовательская Разные права	Подд. к сетям Международного обмена	Подд. к сетям Международного обмена	Однопользовательская	Многопользовательская Равные права	Многопользовательская Разные права	Под к сетям МежОб
1	2	3	4	5	6	7	8	9	10
регистрация попыток доступа программных средств к дополнительным защищаемым объектам доступа (терминалам, техническим средствам, узлам сети, линиям (каналам) связи, внешним устройствам, программам, томам, каталогам, файлам, записям, полям записей). В параметрах регистрации указываются дата и время попытки доступа к защищаемому объекту с указанием ее результата (успешная, неуспешная), идентификатор пользователя, спецификация защищаемого объекта (логическое имя (номер))							+	+	
Обеспечение целостности									
обеспечение целостности программных средств системы защиты персональных данных, обрабатываемой информации, а также неизменность программной среды. При этом целостность программных средств проверяется при загрузке системы по наличию имен (идентификаторов) компонентов **системы** защиты персональных данных, целостность программной среды обеспечивается отсутствием в информационной системе средств разработки и отладки программ	+								

Классы / Требования	3кл/2кл	3кл/2кл	3кл/2кл	3кл	2кл	1кл	1кл	1кл	1кл
	Однопользовательская	Многопользовательская Равные права	Многопользовательская Разные права	Подл. к сетям Международного обмена	Подл. к сетям Международного обмена	Однопользовательская	Многопользовательская Равные права	Многопользовательская Разные права	Под к сетям МежОб
1	2	3	4	5	6	7	8	9	10
обеспечение целостности программных средств системы защиты персональных данных, обрабатываемой информации, а также неизменность программной среды. При этом целостность программных средств проверяется при загрузке системы по наличию имен (идентификаторов) компонентов **средств** защиты информации, а целостность программной среды обеспечивается отсутствием в информационной системе средств разработки и отладки программ						+			
обеспечение целостности программных средств системы защиты персональных данных, обрабатываемой информации, а также неизменность программной среды. При этом целостность программных средств проверяется при загрузке системы по наличию имен (идентификаторов) компонентов системы защиты персональных данных, а целостность программной среды обеспечивается отсутствием в информационной системе средств разработки и отладки программ **во время обработки и (или) хранения защищаемой информации**		+							

Требования \ Классы	3кл/2кл	3кл/2кл	3кл/2кл	3кл	2кл	1кл	1кл	1кл	1кл
	Однопользовательская	Многопользовательская Равные права	Многопользовательская Разные права	Подд. к сетям Международного обмена	Подд. к сетям Международного обмена	Однопользовательская	Многопользовательская Равные права	Многопользовательская Разные права	Под к сетям МежОб
1	2	3	4	5	6	7	8	9	10
обеспечение целостности программных средств системы защиты персональных данных, обрабатываемой информации, а также неизменность программной среды. При этом целостность программных средств проверяется при загрузке системы по **контрольным суммам компонентов средств защиты информации**, а целостность программной среды обеспечивается **использованием трансляторов с языков высокого уровня и отсутствием средств модификации объектного кода программ в процессе обработки и (или) хранения защищаемой информации**			+						
обеспечение целостности программных средств системы защиты персональных данных, обрабатываемой информации, а также неизменность программной среды. При этом целостность системы защиты персональных данных проверяется при загрузке системы по наличию имен (идентификаторов) ее компонент, а целостность программной среды обеспечивается отсутствием в информационной системе средств разработки и отладки программ							+		

Требования \ Классы	3кл/2кл	3кл/2кл	3кл/2кл	3кл	2кл	1кл	1кл	1кл	1кл
	Однопользовательская	Многопользовательская Равные права	Многопользовательская Разные права	Подл. к сетям Международного обмена	Подл. к сетям Международного обмена	Однопользовательская	Многопользовательская Равные права	Многопользовательская Разные права	Под к сетям МежОб
1	2	3	4	5	6	7	8	9	10
обеспечение целостности программных средств системы защиты персональных данных, обрабатываемой информации, а также неизменность программной среды. При этом целостность системы защиты персональных данных проверяется при загрузке системы по **контрольным суммам компонентов системы защиты,** а целостность программной среды обеспечивается использованием трансляторов с языков высокого уровня и отсутствием средств модификации объектного кода программ в процессе обработки и (или) хранения **персональных данных**								+	
физическая охрана информационной системы (технических средств и носителей информации), предусматривающая контроль доступа в помещения информационной системы посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения информационной системы и хранилище носителей информации	+								
физическая охрана информационной системы (**устройств** и носителей информации), предусматривающая контроль доступа в помещения информационной системы посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения информационной системы и хранилище носителей информации		+	+						

Классы / Требования	3кл/2кл	3кл/2кл	3кл/2кл	3кл	2кл	1кл	1кл	1кл	1кл
	Однопользовательская	Многопользовательская Равные права	Многопользовательская Разные права	Подл. к сетям Международного обмена	Подл. к сетям Международного обмена	Однопользовательская	Многопользовательская Равные права	Многопользовательская Разные права	Под к сетям МежОб
1	2	3	4	5	6	7	8	9	10
физическая охрана технических средств информационных систем (устройств и носителей информации), предусматривающая постоянное наличие охраны территории и здания						+	+		
физическая охрана технических средств информационной системы (устройств и носителей информации), предусматривающая контроль доступа в помещения посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения и хранилище носителей информации								+	
периодическое тестирование функций системы защиты персональных данных при изменении программной среды и пользователей информационной системы с помощью тест-программ, имитирующих попытки несанкционированного доступа	+	+	+			+	+	+	
наличие средств восстановления системы защиты персональных данных, предусматривающих ведение двух копий программных компонентов средств защиты информации, их периодическое обновление и контроль работоспособности	+	+	+			+	+	+	
Межсетевое экранирование									
контроль целостности своей программной и информационной части				+	+				+
контроль целостности программной и информационной части межсетевого экрана по контрольным суммам									+

Классы / Требования	3кл/2кл	3кл/2кл	3кл/2кл	3кл	2кл	1кл	1кл	1кл	1кл
	Однопользовательская	Многопользовательская Равные права	Многопользовательская Разные права	Подл. к сетям Международного обмена	Подл. к сетям Международного обмена	Однопользовательская	Многопользовательская Равные права	Многопользовательская Разные права	Под к сетям МежОб
1	2	3	4	5	6	7	8	9	10
фильтрацию пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств				+	+				+
регламентное тестирование реализации правил фильтрации, процесса идентификации и аутентификации администратора межсетевого экрана, процесса регистрации действий администратора межсетевого экрана, процесса контроля за целостностью программной и информационной части, процедуры восстановления				+	+				
регламентное тестирование реализации правил фильтрации, процесса **регистрации, процесса идентификации и аутентификации запросов, процесса** идентификации и аутентификации администратора межсетевого экрана, процесса регистрации действий администратора межсетевого экрана, процесса контроля за целостностью программной и информационной части, процедуры восстановления									+
фильтрацию на сетевом уровне независимо для каждого сетевого пакета (решение о фильтрации принимается на основе сетевых адресов отправителя и получателя или на основе других эквивалентных атрибутов)					+				+
фильтрацию с учетом входного и выходного сетевого интерфейса как средства проверки подлинности сетевых адресов					+				+

Классы / Требования	3кл/2кл	3кл/2кл	3кл/2кл	3кл	2кл	1кл	1кл	1кл	1кл
	Однопользовательская	Многопользовательская Равные права	Многопользовательская Разные права	Подд. к сетям Международного обмена	Подд. к сетям Международного обмена	Однопользовательская	Многопользовательская Равные права	Многопользовательская Разные права	Под к сетям МежОб
1	2	3	4	5	6	7	8	9	10
фильтрацию с учетом любых значимых полей сетевых пакетов					+				+
фильтрацию на транспортном уровне запросов на установление виртуальных соединений с учетом транспортных адресов отправителя и получателя									+
фильтрацию на прикладном уровне запросов к прикладным сервисам с учетом прикладных адресов отправителя и получателя									+
фильтрацию с учетом даты и времени									+
аутентификацию входящих и исходящих запросов методами, устойчивыми к пассивному и (или) активному прослушиванию сети									+
регистрацию и учет фильтруемых пакетов (в параметры регистрации включаются адрес, время и результат фильтрации)					+				+
регистрацию и учет запросов на установление виртуальных соединений									+
локальную сигнализацию попыток нарушения правил фильтрации									+
идентификацию и аутентификацию администратора межсетевого экрана при его **локальных** запросах на доступ по идентификатору (коду) и паролю условно-постоянного действия					+				+
идентификацию и аутентификацию администратора межсетевого экрана при его **удаленных** запросах методами, устойчивыми к пассивному и активному перехвату информации									+

Классы / Требования	3кл/2кл	3кл/2кл	3кл/2кл	3кл	2кл	1кл	1кл	1кл	1кл
	Однопользовательская	Многопользовательская Равные права	Многопользовательская Разные права	Подд. к сетям Международного обмена	Подд. к сетям Международного обмена	Однопользовательская	Многопользовательская Равные права	Многопользовательская Разные права	Под к сетям МежОб
1	2	3	4	5	6	7	8	9	10
предотвращение доступа неидентифицированного пользователя или пользователя, подлинность идентификации которого при аутентификации не подтвердилась									+
регистрацию входа (выхода) администратора межсетевого экрана в систему (из системы) либо загрузки и инициализации системы и ее программного останова (регистрация выхода из системы не проводится в моменты аппаратурного отключения межсетевого экрана)					+				+
регистрацию запуска программ и процессов (заданий, задач)					+				+
регистрацию действия администратора межсетевого экрана по изменению правил фильтрации									+
возможность дистанционного управления своими компонентами, в том числе возможность конфигурирования фильтров, проверки взаимной согласованности всех фильтров, анализа регистрационной информации									+
восстановление свойств межсетевого экрана после сбоев и отказов оборудования									+

Примечание: Для ИСПДн 4 класса перечень мероприятий по защите ПДн определяется в зависимости от ущерба который может быть нанесен в следствии несанкционированного или непреднамеренного доступа к ПДн