Приложение 1

к приказу ОГБУ «МФЦ»

от_____ №_____

ПОЛИТИКА

информационной безопасности

в ОГБУ «МФЦ»

г. Биробиджан, 2016

Оглавление

Введение *3*
Термины и сокращения *3*
1. *Общие положения* *7*
2. *Область действия* *7*
3. *Политика физической безопасности* *7*
4. *Правила эксплуатации электронных устройств* *8*
5. *Политика обеспечения управления доступом* *9*
6. *Политика обеспечения сетевой безопасности* *12*
7. *Построение корпоративной сети Учреждения* *12*
8. *Политика использования программного обеспечения* *13*
9. *Политика парольной защиты* *14*
10. *Политика антивирусной защиты* *16*
11. *Политика использования сети Интернет* *17*
12. *Политика использования электронной почты* *18*
13. *Политика использования отчуждаемых носителей* *20*
14. *Политика использования средств криптографической защиты* *20*
15. *Политика резервного копирования* *21*
16. *Политика работы с бумажными носителями и работы с фотокопировальными устройствами* *22*
17. *Кадровая политика* *23*
18. *Система защиты персональных данных* *24*
19. *Требования к подсистемам СЗПДн* *25*
20. *Пользователи ИСПДн* *28*
21. *Требования к персоналу по обеспечению защиты ПДн* *31*
22. *Должностные обязанности пользователей ИСПДн* *32*
23. *Ответственность работников ИСПДн Учреждения* *32*

Введение

Настоящая Политика информационной безопасности (далее - Политика) разработана в соответствии с целями, задачами и принципами обеспечения безопасности персональных данных ОГБУ «МФЦ» (далее - Учреждение) изложенных в Концепции информационной безопасности ИСПДн Учреждения.

Политика разработана в соответствии с требованиями Федерального закона от 27 июля 2006 г. N 152-ФЗ «О персональных данных» и Постановления Правительства Российской Федерации от 1 ноября 2012 г. N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

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

Термины и сокращения

В настоящем документе используются следующие термины и их определения:

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

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

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

Вредоносный код – содержащаяся в любых файлах последовательность символов, результат исполнения которых позволяет отнести ее к компьютерным вирусам или вредоносным программам.

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 к информации – возможность получения информации и ее использования.

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

Информационная система персональных данных (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.

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.

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.

Корпоративная сеть — это мультисервисная сеть передачи данных, работающая под единым управлением и предназначенная для удовлетворения собственных производственных потребностей организации.

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.

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

Оператор (персональных данных) – государственный орган, муниципальный орган, юридическое или физическое лицо, организующее и (или) осуществляющее обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

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

Персональные данные (ПДн) – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

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

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

Распространение персональных данных – действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом.

Резервное копирование – процесс создания копий рабочей информации на определенный момент времени, направленный на предотвращение нарушения целостности и/или доступности рабочей информации и на ее восстановление после таких нарушений.

Сети общего пользования – любые сети передачи данных (например, Интернет), в которых передаваемая информация может стать известна третьим лицам.

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

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

Угрозы безопасности персональных данных (УБПДн) – 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.

Учреждение – Областное государственное бюджетное Учреждение «Многофункциональный центр предоставления государственных и муниципальных услуг в Еврейской автономной области» и его филиалы

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).

Электронная почта – любое сообщение, изображение, форма, вложение, данные или другое способ представления информации отправляемой, получаемой или хранящейся в системе электронной почты.

1. Общие положения

1.1. Целью настоящей Политики является обеспечение безопасности объектов защиты ИСПДн в ОГБУ «МФЦ» от всех видов угроз, внешних и внутренних, умышленных и непреднамеренных, минимизация ущерба от возможной реализации угроз безопасности ПДн (УБПДн) информационной системы.

1.2. 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.

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

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

1.5. Состав объектов защиты представлен в Перечне персональных данных обрабатываемых в Учреждении, утверждаемом Руководителем Учреждения.

2. Область действия

2.1. Требования настоящей Политики распространяются на всех работников Учреждения, а также всех прочих лиц, допущенных к работам на территории Учреждения (подрядчики, аудиторы и т.п.).

3. Политика физической безопасности

3.1. Помещения, которые должны быть оборудованы дополнительными устройствами регистрации, контроля и поддержания заданных характеристик (например, система автоматического пожаротушения, контроля влажности, принудительной вентиляции, кондиционирования воздуха, защиты от статического электричества и т.п.), в соответствии с НПА РФ или правилами эксплуатации оборудования, размещенного в таких помещениях, и требуемых для соблюдения гарантийных обязательств производителя, должны быть полностью укомплектованы подобными устройствами.

3.2. В помещениях, в которых размещается имущество Учреждения, должна иметься возможность организации круглосуточной охраны. В помещениях, расположенных в зданиях, в которых возможно использование услуг служб централизованной охраны здания, охрана должна осуществляться силами таких служб. В помещениях, расположенных в зданиях без служб централизованной охраны, охрана должна осуществляться за счет привлечения специализированных организаций, предоставляющих услуги по круглосуточной охране. Допускается в рабочее время

использование услуг служб охраны в режиме «вызов по необходимости», в нерабочее время помещения должны сдаваться под охрану с применением средств охранной сигнализации или с физическим наблюдением за помещениями.

3.3. Периметр зданий, в которых располагаются помещения Учреждения, должен охраняться посредством систем видеонаблюдения с возможностью хранения информации, а также вывода информации на пульт в помещении охраны.

3.4. Все помещения Учреждения должны быть оборудованы дверьми, закрываемыми на замок.

3.5. Должен быть предусмотрен механизм установления личности осуществляющей санкционированное вскрытие помещений Учреждения (например, проверка удостоверения личности, применение систем контроля и управления доступом, роспись за получения ключа от помещений на посту охраны и т.п.).

3.6. Отдельные группы помещений, нахождение в которых посторонних лиц не требуется (например, архивные помещения), могут отделяться дополнительными дверьми, иными средствами ограничения доступа, опечатываться или физически располагаться удаленно (например, на других этажах или частях здания и т.п.).

3.7. Доступ в помещения Учреждения и его филиалов, где хранятся и обрабатываются персональные данные, осуществляется в соответствии Перечнем должностей работников ОГБУ «МФЦ», замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным, который утверждается Руководителем Учреждения.

3.8. Работники Учреждения не должны оставлять свои рабочие кабинеты без наблюдения. В случае, если помещение остается без наблюдения, помещение должно быть закрыто на замок.

3.9. Работники Учреждения не должны пытаться проникнуть в помещения, доступ к которым ограничен, не имея на это соответствующих прав.

3.10. Нахождение посетителей или представителей сторонних организаций в помещениях Учреждения, должно контролироваться сопровождающими лицами из числа работников Учреждения, допущенных в данные помещения в соответствии с пунктом 3.6. или охранником.

3.11. Работники сторонних организаций должны вызываться в установленном порядке. При приходе таких работников без предварительной заявки их допуск в помещения Учреждения должен осуществляться только по согласованию с ответственным лицом структурного подразделения Учреждения, в ведении которого предполагаются проводимые работы. Работники сторонних организаций должны находиться на территории Учреждения в сопровождении уполномоченных работников Учреждения.

4. Правила эксплуатации электронных устройств

4.1. Размещение экранов АРМ, обрабатывающих информацию ограниченного доступа, должно исключать возможность их просмотра лицами, не допущенными к данной информации.

4.2. При использовании систем видеонаблюдения, такие системы должны быть установлены в местах, исключающих просмотр содержимого экранов АРМ, обрабатывающих информацию ограниченного доступа, а также исключающих просмотр вводимых паролей, кодов и т.п.

4.3. Системные блоки АРМ, периферийное оборудование должно быть опечатано или оборудовано иным способом ограничения их несанкционированного вскрытия.

4.4. Работникам Учреждения запрещено подключать или устанавливать собственные компьютеры, периферийные устройства, в том числе съемные носители информации, комплектующие к АРМ и корпоративной сети Учреждения без согласования с администратором безопасности Учреждения или лицом его заменяющим.

4.5. Все электронные устройства должны проходить профилактическое обслуживание. Такое обслуживание должно проводиться регулярно, но не реже сроков, указанных в технической документации на устройства или нормативных актах Учреждения. Профилактическое обслуживание должно производиться силами квалифицированных работников Учреждения, если иное не определено производителем оборудования.

4.6. Все АРМ, предназначенные для выполнения работниками своих должностных обязанностей, должны быть оборудованы источниками бесперебойного питания.

4.7. Сетевые, питающие и иные кабеля должны быть проложены с соблюдением стандартов и должно быть исключено повреждение таких кабелей при повседневной работе, а также минимизировать вероятность получения травмы работниками Учреждения, вызванных нарушениями укладки таких кабелей.

4.8. Перед передачей (в том числе для ремонта) сторонним организациям, списанием или прекращением использования оборудования, участвовавшего в обработке информации ограниченного доступа, должна быть проведена проверка, с целью исключения попадания такой информации третьим лицам.

5. Политика обеспечения управления доступом

5.1. Работникам Учреждения запрещено осуществление противоправных действий, включая деятельность по получению несанкционированного доступа к любой АС; нанесение ущерба и нарушение работы АС; перехват паролей или иной способ получения паролей, ключевой информации или иных механизмов доступа, которые могут быть использованы для несанкционированного доступа.

5.2. Программное обеспечение, предполагающее использование механизмов разделения доступа или подразумевающее индивидуальную ответственность работника за осуществляемые действия, должно использовать механизм контроля доступа, с идентификацией и авторизацией пользователя с помощью, как минимум пароля, отвечающего требованиям политики парольной защиты.

5.3. Настройка доступа ко всем информационным ресурсам Учреждения должна быть по умолчанию направлена на предотвращение к ним любого несанкционированного доступа.

5.4. Если система контроля доступа АРМ, корпоративной сети или автоматизированной системе вышла из строя, то по умолчанию доступ пользователей должен быть запрещен.

5.5. Доступ к информационным ресурсам Учреждения должен осуществляться согласно разработанной и утвержденной руководителем «Матрицы доступа», составленной на основании должностных обязанностей работников Учреждения и отчета о проведенной внутренней проверки.

5.6. Любое изменение в правах доступа к информационным ресурсам Учреждения должно быть обосновано выполнением должностных обязанностей, утверждено и направлено администратору информационной безопасности.

5.7. При увольнении работников Учреждения или изменении их должностных обязанностей, лица, уполномоченные на предоставление прав доступа, должны быть письменно проинформированы в трехдневный срок, после чего внести соответствующие изменения в систему контроля доступа и «Матрицу доступа».

5.8. Для установления персональной ответственности идентификатор учетной записи пользователя в любой информационной системе должен однозначно соответствовать отдельному работнику.

5.9. Компьютеры и терминалы должны быть оставлены в состоянии выполненного выхода из системы или с запирающим механизмом экрана или клавиатуры, управляемым паролем, маркером или подобным механизмом аутентификации пользователя, когда они находятся без присмотра, и должны быть защищены блокировкой клавиатуры, паролями или другими средствами управления, когда не используются.

5.10. Для доступа к АРМ и корпоративной сети Учреждения у каждого пользователя должны быть уникальный набор из идентификатора учетной записи и пароля. Запрещено создание идентификатора учетной записи, используемого группой лиц.

5.10.1. Использование идентификатора учетной записи пользователя после увольнения или прекращения использования информационных ресурсов Учреждения запрещено.

5.10.2. При предоставлении идентификатора учетной записи сторонним организациям необходимо заключение соглашений, подтверждающих обязательства сторонних организаций соблюдать требования НПА РФ и организационно-распорядительных документов Учреждения, подписанные уполномоченными лицами.

5.10.3. При прекращении необходимости использования сторонними организациям идентификатора учетной записи, лица, уполномоченные на предоставление прав доступа, должны быть письменно проинформированы в однодневный срок, после чего должны быть внесены соответствующие изменения в систему контроля доступа и «Матрицу доступа».

5.10.4. Для всех лиц, не являющихся служащими Учреждения, но для выполнения обязательств которых, необходимо предоставление доступа к АРМ и корпоративной сети Учреждения, должен быть сформирован идентификатор учетной записи, действующий только на период выполнения лицом своих обязательств. В случае, если срок выполнения обязательств не определен, то срок действия идентификатора учетной записи должен составлять 60 дней.

5.10.5. Пользователям запрещено использование идентификаторов учетных записей и паролей, используемых для получения доступа к информационным ресурсам Учреждения, для идентификации и аутентификации на публичных ресурсах сетей общего пользования.

5.11. Все автоматизированная системы и технические средства должны поддерживать специальный тип учетной записи, позволяющий производить любые поддерживаемые настройки и изменения, включая изменения в системе обеспечения безопасности.

5.11.1. Количество таких типов учетных записей должно быть максимально ограничено и предоставлено только тем пользователям, которым это необходимо для осуществления должностных обязанностей с учетом соблюдения требований НПА РФ и организационно-распорядительных документов Учреждения.

5.11.2. Таким лицам должны быть предоставлены как минимум два типа учетных записей, одна – специальный тип учетной записи, другая – ограниченный тип учетной записи для повседневной работы, не требующей изменения настроек АС.

5.11.3. Удаленное администрирование любых технических устройств в корпоративной сети Учреждения, при котором осуществляется передача информации через сети общего пользования, запрещено.

5.12. АРМ должны переводиться в режим запроса пароля после определенного периода бездействия или при отсутствии возможности контроля пользователем доступа к АРМ.

5.12.1. При наличии технической возможности, средства контроля доступа должны быть настроены на временную блокировку доступа к ним, после трехкратной попытки получения доступа, и уведомления уполномоченных лиц о таковых фактах.

5.12.2. При наличии технической возможности удаленные подключения к автоматизированной системе должны автоматически отключаться после определенного времени неактивности такого подключения.

5.13. Пользователям запрещено собирать и копировать информацию с информационных ресурсов, если это не обусловлено выполнением должностных обязанностей. При наличии технической возможности используемые системы контроля доступа должны предупреждать возможность таких действий и информировать о таких попытках.

5.14. Программисты и другой технический персонал не должны устанавливать и использовать программное обеспечение, направленное на обход установленных механизмов доступа или получение сведений для несанкционированного доступа. Если использование такого программного обеспечения необходимо для выполнения должностных обязанностей, то его использование должно осуществляться только уполномоченными лицами.

6. Политика обеспечения сетевой безопасности

6.1. Конфигурация и настройка всех устройств подключенных к корпоративной сети Учреждения должны соответствовать требованиям НПА РФ и организационно-распорядительным документам Учреждения.

6.2. Размещение в корпоративной сети Учреждения информации ограниченного доступа должно соответствовать требованиям НПА РФ и организационно-распорядительным документам Учреждения.

6.3. Используемые внешние интерфейсы и протоколы корпоративной сети Учреждения должны быть максимально ограничены необходимыми для обеспечения выполнения Учреждением своих задач и функций.

6.4. Технические средства, обеспечивающие работу корпоративной сети, должны размещаться с соблюдением требований по контролю физического доступа к ним и организации их сохранности. Доступ в помещения лиц, не уполномоченных для работы с данным оборудованием, должен быть исключен или осуществляться в сопровождении уполномоченных работников Учреждения.

6.5. Для управления техническими устройствами в сети по возможности должны быть использован протоколы поддерживающие криптографическую защиту информации.

7. Построение корпоративной сети Учреждения

7.1. Построение корпоративной сети должно исключать наличие «узких мест», нарушение работы которых приведет к нарушению работы всей корпоративной сети.

7.2. Все корпоративные сети Учреждения должны быть настроены для недопущения несанкционированного подключения к ним и обнаружения попыток таких подключений.

7.3. Подключение к корпоративной сети Учреждения разрешено только после выполнения требований политик безопасности и критериев, определенных Учреждением.

7.4. Доступ к информации о системе внутренней адресации в корпоративной сети, конфигурации и иной подобной информации должен быть обусловлен только выполнением должностных обязанностей. В отдельных случаях, подобная информация может предоставляться третьим лицам, для проведения работ в рамках договорных обязательств. При этом между сторонами должно быть заключено соглашение о конфиденциальности.

7.5. Использование любого типа подключений (DSL-модем, dial-up модем, модемы, использующие сети Операторов мобильной связи и т.п.) технических средств, размещенных в корпоративной сети Учреждения, к внешним информационным ресурсам, запрещено без согласования с уполномоченными лицами. Такие подключения должны соответствовать требованиям НПА РФ и организационно-распорядительным документам Учреждения.

7.6. Настройка маршрутизаторов должна осуществляться в соответствии с рекомендациями производителя, обеспечивающими максимальный уровень безопасности.

7.7. Доступ к программным настройкам активных технических средств корпоративной сети должен быть ограничен паролем, отвечающим требованиям политики парольной защиты Учреждения.

7.8. Добавление прав правил маршрутизации должно осуществляться на основании политик безопасности Учреждения и позволять решать задачи и функции, возложенные на Учреждение. Правила маршрутизации должны быть утверждены руководителем Учреждения и находиться у лица, уполномоченного на администрирование корпоративной сети.

7.9. Пользователям запрещен просмотр информационных ресурсов Учреждения, содержащихся на АРМ других пользователей или в корпоративной сети Учреждения, если это не обусловлено выполнением должностных обязанностей.

8. Политика использования программного обеспечения

8.1. Программное обеспечение, используемое для осуществления деятельности структурных подразделений Учреждения, должно соответствовать условиям его лицензирования (независимо от того, является ли оно коммерческим или свободно распространяемым) и использоваться строго в соответствии с лицензионным соглашением. Любое структурное подразделение Учреждения должно исключить случаи хранения и/или использования программного обеспечения, не являющегося лицензионным.

8.2. В случае если в НПА РФ предъявляются особые требования к программному обеспечению (например, требование по сертификации такого программного обеспечения уполномоченными организациям и т.п.) структурное подразделение Учреждения обязано обеспечить выполнение подобных требований.

8.3. На каждое АРМ должен быть установлен комплект программного обеспечения, необходимый и достаточный для выполнения на нем поставленных задач.

8.4. Учреждение предоставляет работникам достаточное количество лицензий на использование программного обеспечения, необходимого для выполнения должностных обязанностей.

8.5. На технические средства, подключаемые к корпоративной сети Учреждения и подразумевающие возможность установки программного обеспечения, должно быть установлено базовое программное обеспечение, предусмотренное «Перечнем программного обеспечения, разрешенного к установке на технических средствах, подключаемых к корпоративной сети Учреждения».

8.6. Обновление версий программного обеспечения, использующего ресурсы КС, должно осуществляться только администраторами автоматизированных систем или уполномоченным лицом. Допустимо использование функции автоматического обновления программного обеспечения, использующего ресурсы корпоративной сети Учреждения.

8.7. Пользователям запрещено выполнение команд уровня операционной системы или предпринимать попытки их выполнения. Действия пользователя должны быть ограничены взаимодействием с элементами экранных форм программного обеспечения, необходимым для выполнения должностных обязанностей.

8.8. При увольнении или изменении должностных обязанностей пользователя, файлы, содержащиеся на его АРМ, должны быть проверены его непосредственным руководителем и, в случае необходимости, переданы другим исполнителям.

9. Политика парольной защиты

9.1. Доступ к программному обеспечению, используемому пользователями и администраторами в рамках должностных обязанностей и подразумевающему наличие идентификации и аутентификации пользователя и/или разграничение полномочий без использования пароля запрещено.

9.2. Пароли доступа к различному прикладному программному обеспечению, используемому пользователями и администраторами в рамках должностных обязанностей должны отличаться от паролей доступа к автоматизированному рабочему месту или элементам сетевой инфраструктуры и не должны совпадать для различного программного обеспечения.

9.3. Создание пароля должно предусматривать создание первичного пароля администратором, с последующей его сменой пользователем при первом запуске программного обеспечения. В случае если данная возможность не поддерживается программным обеспечением, пользователь обязан самостоятельно создать пароль пользователя при первом запуске программного обеспечения.

9.4. Пароли не должны передаваться в электронных сообщениях или любых иных формах электронного обмена.

9.5. Системные пароли (например, пароль учетной записи Root, администратор, а также пароли обеспечивающие возможность полного управления и настройки (включая изменения прав доступа) используемым в Учреждении программным обеспечением) должны меняться регулярно, но не реже одного раза в три месяца.

9.6. Пароли пользователей (например, пароли учетной записи, удаленного доступа к базам данным) должны меняться регулярно, но не реже одного раза в три месяца, если иное не определено НПА РФ и/или организационно-распорядительными документами Учреждения.

9.7. В случае компрометации пароля необходимо его немедленное изменение, а также оповещение о данном факте администратора информационной безопасности.

9.8. Внеплановая смена паролей пользователя производится в случае прекращения или изменения его полномочий (переход на другую работу внутри Учреждения и т.п.) немедленно после окончания последнего сеанса работы данного пользователя с системой.

9.9. Полная внеплановая смена всех системных паролей и паролей пользователей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу внутри Учреждения и т.п.) любого из лиц, выполнявших должностные обязанности администратора и/или имевшего доступ к таким паролям.

9.10. Восстановление утерянных паролей пользователей осуществляется администратором, путем сброса забытого пароля и установления первичного пароля, в случае если установка первичного пароля не поддерживается программным обеспечением, администратор осуществляет сброс забытого пароля, а пользователь обязан самостоятельно создать пароль пользователя при первом запуске программного обеспечения. Основанием для смены пароля может являться только заявка в письменной форме.

9.11. Пользователи не должны сообщать свои пароли третьим лицам, включая руководителей и лиц, осуществляющих сопровождение программного обеспечения. Администраторы автоматизированных систем не должны просить пользователей сообщить им их пароли.

9.12. Хранение пользователями любых паролей в электронном или физическом виде на любом, в том числе личном, носителе информации (в виде отдельных файлов, записей в ежедневниках, а также с применением функций программного обеспечения и т.п.), разрешено при условии исключения возможности получения доступа к паролям третьих лиц.

9.13. Хранение паролей администраторами (в том числе администраторами информационной безопасности), допускается при применении средств криптографической защиты, при этом хранение не зашифрованных системных паролей в электронном виде – запрещено. Использование администраторами функций программного обеспечения, позволяющих исключить ввод пароля при повторных запусках, возможно в исключительных случаях (например, в системе резервного копирования, системе антивирусной защиты).

9.14. Допускается хранение пароля на индивидуальном носителе (электронный идентификатор touch memory и т.д.). В таком случае пользователь несет персональную ответственность за сохранность данного индивидуального носителя, а также обязуется вернуть его по запросу структурного подразделения Учреждения, выдавшего его, или при прекращении полномочий.

10. Политика антивирусной защиты

10.1. Антивирусное программное обеспечение должно быть установлено и функционировать в штатном режиме на всех компьютерах, выполняющих функции серверов корпоративной сети Учреждения, на всех АРМ отдельно стоящих и подключенных к корпоративной сети и на всех портативных компьютерах.

10.2. Не допускается изменение настроек системы антивирусной защиты, в части оповещения о нахождении компьютерных вирусов или вредоносных программ, в результате действия которых уменьшается эффективность работы АС.

10.3. Обновления баз системы антивирусной защиты должно производиться регулярно. Построение системы антивирусной защиты должно предусматривать возможность обновления ее антивирусных баз и компонентов производителем по мере их создания. В случае невозможности такого построения системы (например, отдельно стоящие АРМ не подключенные к каким-либо сетям), обновление системы антивирусной защиты должно производиться с регулярностью, обеспечивающей ее эффективное функционирование.

10.4. Запрещается отключение системы антивирусной защиты, за исключением случаев проведения тестирования программного обеспечения и иных тестов, проводимых уполномоченными работниками Учреждения.

10.5. Структурные подразделения Учреждения обязаны проводить сканирование своих информационных ресурсов, а также всех подключенных АРМ на наличие компьютерных вирусов и/или вредоносных программ.

10.6. Файлы, полученные любым образом, с любых носителей информации или сетей общего пользования должны быть проверены на наличие вредоносного кода.

10.7. Подключения к АРМ незарегистрированных отчуждаемых носителей информации (дискеты, компакт-диски, съемные жесткие диски, сотовые телефоны, карманные персональные компьютеры, фотоаппараты и иные носители информации) разрешено с обязательной проверкой «по требованию» таких носителей информации на наличие компьютерных вирусов и/или вредоносных программ.

10.8. В случае получения файлов, проверка которых в исходном состоянии невозможна (например, файлы содержат архивы, не поддерживаемые системой антивирусной защиты, файлы прошли криптографическое преобразование и т.п.), необходимо на АРМ, не подключенном к корпоративной сети Учреждения, привести данные файлы к состоянию пригодному для проверки на наличие вредоносного кода, осуществить такую проверку, после чего принимать решение о возможности использования данных файлов.

10.9. Все файлы передаваемые третьим лицам должны быть проверены на наличие вредоносного кода системой антивирусной защиты до их передачи.

10.10. Любые намеренные попытки написания, компиляции, хранения, запуска, пропагандирования или распространения пользователями компьютерных вирусов или вредоносных программ, а также иного кода, предназначенного для саморазмножения, нанесения ущерба или снижения производительности автоматизированных систем Учреждения, запрещены.

10.11. В случае обнаружения системой антивирусной защиты компьютерного вируса или вредоносной программы пользователь обязан прекратить работу и сообщить об этом администратору информационной безопасности.

10.12. О любом инциденте, связанном с выявлением компьютерного вируса или вредоносных программ, на АРМ или портативном компьютере, подключаемом к корпоративной сети Учреждения, должно быть сообщено администратору информационной безопасности.

10.13. Самостоятельные попытки пользователя по удалению компьютерного вируса или вредоносной программы запрещены.

11. Политика использования сети Интернет

11.1. Вся информация, полученная из сети Интернет, должна считаться недостоверной, не будучи подтвержденной из других источников. Перед использованием свободно распространяемой информации из сети Интернет для принятия решений в рамках деятельности Учреждения, такая информация должна быть перепроверена в других источниках.

11.2. Учреждение не несет ответственности за информацию, содержащуюся в сети Интернет. В случае открытия пользователем ресурсов, содержание которых может считаться незаконным или оскорбительным пользователь обязан прекратить работу с данным ресурсом.

11.3. Для получения возможности доступа пользователя в сети Интернет должны быть обеспечены механизмы защиты информационных ресурсов Учреждения от воздействия из сети Интернет.

11.4. Передача информации ограниченного доступа по сетям общего пользования, допускается при условии соблюдения всех требований к такой передаче. Передача информации ограниченного доступа без соблюдения требований, предъявляемых к ее передаче по сети Интернет, запрещена.

11.5. Пользователю запрещено любое тестирование и/или попытки обхода установленных механизмов защиты информационных ресурсов Учреждения.

11.6. Запрещено предоставлять доступ к сети Интернет стороннему обслуживающему персоналу, консультантам и иным лицам, состоящим в договорных отношениях с Учреждением, за исключением случаев, когда такой доступ необходим для решения данными лицами задач в интересах структурных подразделений Учреждения. Доступ может быть предоставлен только по согласованию с уполномоченным лицом структурного подразделения Учреждения, а в случае использования корпоративной сети Учреждения – с администратором информационной безопасности.

11.7. Использование сети Интернет для личных нужд пользователя запрещен. Доступ пользователям предоставляется к сети Интернет для выполнения должностных обязанностей. Использование сети Интернет для участия в игровых, развлекательных и иных ресурсах (включая конкурсы, выставки, социальные сети и иные Интернет-сообщества) запрещено.

11.8. Пользователям запрещена загрузка любого программного обеспечения из сети Интернет. В исключительных случаях, когда загрузка такого программного обеспечения продиктована соблюдением интересов Учреждения, загрузка программного обеспечения из сети Интернет осуществляется уполномоченными лицами структурных подразделений Учреждения.

11.9. Пользователям Учреждения запрещено участвовать в обмене пиратским программным обеспечением, серийными номерами программного обеспечения и ином обмене, нарушающем и/или ущемляющем права правообладателей обмениваемой информации.

12. Политика использования электронной почты

12.1. Электронная почта должна быть использованы работниками Учреждения только для выполнения должностных обязанностей, выполнения договорных обязательств Учреждения и выполнения требований НПА РФ.

12.2. Запрещено использовать электронную почту для отправления писем следующего содержания:

1) писем, содержащих конфиденциальную информацию, в том числе персональные данные, обрабатываемые и охраняемые в Учреждении

2) писем, содержание которых может считаться незаконным или оскорбительным, например, материалы сексуального характера, расистские, дискредитирующие, оскорбительные, непристойные, уничижительные, дискриминационные, угрожающие, или иные подобные сообщения;

3) любых подрывных, оскорбительных, неэтичных, незаконных или недопустимых материалов, включая оскорбительные комментарии по поводу расы, пола, цвета, инвалидности, возрасте, сексуальной ориентации, порнографии, терроризма, религиозных убеждений и верований, политических убеждений или о национальном происхождении, гиперссылок или других ссылок на неприличные или очевидно оскорбительные веб-сайты и подобные материалы, шутки, массовые рассылки, предупреждений о вирусах и розыгрышей, обращений о помощи или вредоносного кода;

4) писем, написанных таким образом, который может быть интерпретирован как официальная позиция или высказывание Учреждения, если это не разрешено руководителем Учреждения в соответствии с нормативно-методическими документами Учреждения.

12.3. Запрещено использовать электронную почту в следующих целях:

1) отправки сообщения с чужого почтового ящика или от чужого имени;

2) отправки сообщений в личных или благотворительных целях, не связанных с деятельностью Учреждения;

3) отправки и пересылки писем, пересылаемых по цепочке («письма счастья»);

4) массовой рассылки писем, кроме случаев, когда необходимо оповещение большого числа работников Учреждения или в случаях когда это обусловлено выполнением задач Учреждения;

5) в любых других незаконных, неэтичных и неразрешенных целях.

12.4. Работники Учреждения, получившие электронную почту от другого пользователя Учреждения, с сообщениями, содержащими запрещенное содержание обязаны уведомить о таком факте администратора информационной безопасности.

12.5. Использование электронной почты должно осуществляться с применением технологий идентификации и аутентификации пользователя.

12.6. Отправка электронной почты, содержащей информацию ограниченного доступа, должна осуществляться в соответствии с требованиями, предъявляемыми к такой информации.

12.7. Пользователям запрещено открывать вложения в электронные сообщения, в случае если отправитель данного сообщения не известен пользователю. Открывать вложения от неизвестных отправителей допускается только администраторам.

12.8. Пользователям запрещено отвечать на запросы любой персональной идентификационной информации, включая пароли, коды доступа, номера кредитных карт и т.п. В случае получения сообщений с такими запросами пользователь обязан сообщить о них администратору информационной безопасности.

13. Политика использования отчуждаемых носителей

13.1. Использование личных отчуждаемых носителей информации запрещено для всех работников Учреждения. На АРМ пользователей программно-аппаратными средствами должен быть ограничен доступ к отчуждаемым носителям информации.

13.1. Работники, которым необходимо использование отчуждаемых носителей информации для выполнения должностных обязанностей, должны быть обеспечены Учреждением такими носителями.

13.2. Служебные отчуждаемые носители информации должны подлежать учету, а их передача работникам должна быть подтверждена их росписью. Работник несет персональную ответственность за их сохранность. Работникам запрещено создавать предпосылки для осуществления утраты, кражи и иных противоправных действий со служебными отчуждаемыми носителями информации.

13.3. Использование отчуждаемых носителей информации для хранения информации ограниченного доступа должно соответствовать требованиям НПА РФ и внутренних документов Учреждения.

13.4. Использование служебных отчуждаемых носителей информации в личных целях запрещено.

13.5. Подключение служебных отчуждаемых носителей информации к техническим средствам, заведомо содержащим вирусы и/или вредоносные программы, запрещено. В этом случае отчуждаемые носители передаются администратору информационной безопасности.

13.6. Эксплуатация отчуждаемых носителей информации должна осуществляться в соответствии с требованиями по их эксплуатации, и направлена на предупреждение их неисправности.

14. Политика использования средств криптографической защиты

14.1. Деятельность со средствами криптографической защиты должны исключать нарушение законодательства Российской Федерации в области лицензирования. В случае, если предполагаемая деятельность со средствами криптографической защиты подразумевает необходимость получения лицензии, то Учреждение обязано получить такую лицензию или привлекать для подобной деятельности сторонние организации, имеющие соответствующие лицензии.

14.2. При использовании средств криптографической защиты для защиты информации ограниченного доступа данные криптографические средства должны соответствовать требованиям НПА РФ.

14.3. Установка, настройка и техническое сопровождение средств криптографической защиты должно осуществляться квалифицированными специалистами и не нарушать требования НПА РФ.

14.4. Использование, в том числе хранение, средств криптографической защиты должно отвечать требованиям законодательства Российской Федерации.

14.5. Перед использованием средств криптографической защиты работники обязаны пройти обучение по порядку их использования.

14.6. Пользователям запрещено использование средств криптографической защиты других пользователей, в том числе с целью выдать себя за другого пользователя.

14.7. Все действия по обеспечению сохранности ключей должны быть направлены на исключение компрометации ключей.

14.8. В случае компрометации ключей или подозрения на компрометацию пользователь обязан прекратить любое использование средств криптографической защиты и незамедлительно сообщить о данном факте уполномоченному лицу Учреждения.

15. Политика резервного копирования

15.1. Резервное копирование информации, размещенной на АРМ пользователей и компьютерах, выполняющих функции сервера КС, осуществляется уполномоченным лицом Учреждения.

15.2. Политика резервного копирования распространяется только на рабочую информацию, хранящуюся на информационных ресурсах Учреждения.

15.3. Резервное копирование должно сочетать как минимум две технологии резервного копирования, одной из которых должна быть технология RAID, используемая для создания дисковых массивов на аппаратных ресурсах Учреждения.

15.4. Регулярность создания резервных копий рабочей информации должна быть достаточной для продолжения нормальной работы Учреждения, в случае нарушения целостности и/или доступности рабочей информации на информационных ресурсах Учреждения, но не реже одного раза в день для ежедневно изменяющихся данных и одного раза в неделю для периодически изменяющихся данных. Копирование резервных копий на отчуждаемые носители (внешние дисковые хранилища и т.п.) должно осуществляться регулярно, но не реже одного раза в месяц.

15.5. Все резервные копии, должны быть размещены в отдельных каталогах, название которых отражает дату последнего изменения рабочей информации и ее краткое описание.

15.6. Вся рабочая информация, хранящаяся на аппаратных ресурсах Учреждения и регулярно копируемая на отчуждаемые носители, должна быть доступна для дальнейшего восстановления.

15.7. Как минимум одна резервная копия рабочей информации должна храниться на отчуждаемом носителе.

15.8. Процессы резервного копирования и восстановления для каждого отдельного типа информации должны быть документированы и периодически пересматриваться.

15.9. Для хранения резервных копий на отчуждаемых носителях должны выбираться такие отчуждаемые носители, характеристики которых не изменяются в течение предполагаемого времени хранения резервных копий.

15.10. Хранение резервных копий рабочей информации на отчуждаемых носителях должно осуществляться с организацией контролируемого доступа к данным носителям, их защитой от воздействия окружающей среды и в разных помещениях с компьютерами, выполняющими функции сервера в корпоративной сети Учреждения.

15.11. Порядок хранения резервных копий информации ограниченного доступа определяется отдельными требованиями по защите информации ограниченного доступа.

15.12. Срок хранения резервных копий на внешних носителях определяется регламентом резервного копирования, если иное не определено НПА РФ, или организационно-распорядительными документами Учреждения.

15.13. Резервные копии, хранящиеся более полугода, должны ежеквартально тестироваться, для подтверждения возможности их восстановления и использования.

16. Политика работы с бумажными носителями и работы с фотокопировальными устройствами

16.1. Конфиденциальная информация, например, на бумажном или на электронном носителе, должна быть заперта (в сейфе, в шкафу или на полках в специальном помещении для хранения), если она не требуется, особенно в нерабочее время.

16.2. Пункты работы с входящей и исходящей почтой и факсимильные аппараты, находящиеся без присмотра, должны быть защищены.

16.3. Неразрешенное использование фотокопировальных устройств и другой техники воспроизведения (например, сканеры, цифровые камеры), должно предотвращаться.

16.4. Документы, содержащие конфиденциальную информацию, должны удаляться с принтеров немедленно.

17. Кадровая политика

17.1. Претендентам на работу не должна раскрываться информация об имеющейся системе защиты информации.

17.2. До начала выполнения своих должностных обязанностей до претендента должна быть доведена вся необходимая информация и проведены все инструктажи в соответствии с требованиями НПА РФ и организационно-распорядительной документации Учреждения.

17.3. Ответственное выполнение требований по информационной безопасности является обязанностью всех работников Учреждения. Требования по информационной безопасности касаются всех работников Учреждения.

17.4. Для выполнения требований по информационной безопасности работники должны знать требования НПА РФ и организационно-распорядительной документации Учреждения, регламентирующие данные требования и письменно подтверждать свое согласие на их выполнение.

17.5. В зависимости от должностных обязанностей, знание требований по информационной безопасности могут быть включены в программу проведения аттестации персонала.

17.6. Не выполнение требований НПА РФ и организационно-распорядительной документации Учреждения по защите информации является поводом для проведения служебных расследований и возможному привлечению к дисциплинарной, административной и уголовной ответственности в соответствии с действующим законодательством Российской Федерации и административно-правовыми нормами, установленными в Учреждения.

17.7. Для выполнения требований по информационной безопасности пользователям запрещено прибегать к помощи третьих лиц, без согласования с руководителем Учреждения или своего филиала.

17.8. При увольнении или прекращении договорных обязательств работники должны быть уведомлены и согласны с требованиями по неразглашению информации ограниченного доступа и сведений о системе защиты информации в Учреждении, в соответствии с НПА РФ и организационно-распорядительной документацией Учреждения.

18. Система защиты персональных данных

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

- Перечня персональных данных, подлежащих защите;

- Акта классификации информационной системы персональных данных;

- Модели угроз безопасности персональных данных;

- Руководящих документов ФСТЭК и ФСБ России.

18.2. На основании этих документов определяется необходимый уровень защищенности ПДн каждой ИСПДн Учреждения. На основании анализа актуальных угроз безопасности ПДн, описанного в Модели угроз, и Акта о результатах проведения проверки 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.

18.3. Для каждой 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.

18.4. 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.

18.5. 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.

18.6. 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 руководителем Учреждения или лицом, ответственным за обеспечение защиты ПДн.

19. Требования к подсистемам СЗПДн

19.1. 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.

19.2. Подсистемы СЗПДн имеют различный функционал в зависимости от класса ИСПДн, определенного в Акте классификации информационной системы персональных данных.

19.3. 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 регистрация 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.

19.4. 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.

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

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

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

19.8. Средства антивирусной защиты предназначены для реализации следующих функций:

- резидентный антивирусный мониторинг;

- антивирусное сканирование;

- скрипт-блокирование;

- централизованная/удаленная установка/деинсталляция антивирусного продукта, настройку, администрирование, просмотр отчетов и статистической информации по работе продукта;

- автоматизированное обновление антивирусных баз;

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

- автоматический запуск сразу после загрузки операционной системы.

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

19.10. Подсистема межсетевого экранирования предназначена для реализации следующих функций:

- фильтрация открытого и зашифрованного (закрытого) IP-трафика;

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

- идентификация и аутентификация администратора межсетевого экрана при его локальных запросах на доступ;

- регистрация входа (выхода) администратора межсетевого экрана в систему (из системы) либо загрузки и инициализации системы;

- контроль целостности своей программной и информационной части;

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

- фильтрация с учетом входного и выходного сетевого интерфейса для проверки подлинности сетевых адресов;

- регистрация и учет запрашиваемых сервисов прикладного уровня;

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

- контроля за сетевой активностью приложений и обнаружения сетевых атак.

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

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

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

19.14. Подсистема обнаружения вторжений, должна обеспечивать выявление сетевых атак на элементы ИСПДн подключенные к сетям общего пользования и (или) международного обмена.

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

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

19.17. Подсистема реализуется внедрением криптографических программно-аппаратных комплексов.

20. Пользователи ИСПДн

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

20.2. В ИСПДн Учреждения можно выделить следующие группы пользователей, участвующих в обработке и хранении ПДн:

- Администратора ИСПДн;

- Администратора информационной безопасности (ИБ);

- Оператора АРМ;

- Администратора корпоративной сети (КС);

- Технического специалиста по обслуживанию периферийного оборудования;

- Программист-разработчик ИСПДн.

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

20.4. Администратор ИСПДн - работник Учреждения, ответственный за настройку, внедрение и сопровождение ИСПДн. Обеспечивает функционирование подсистемы управления доступом ИСПДн и уполномочен осуществлять предоставление и разграничение доступа конечного пользователя (АРМ) к элементам, хранящим персональные данные.

20.4.1. 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.

20.5. Администратор информационной безопасности - работник Учреждения, ответственный за функционирование СЗПДн, включая обслуживание и настройку административной, серверной и клиентской компонент СЗПДн.

20.5.1. Администратор информационной 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).

20.5.2. 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;

- устанавливать доверительные отношения своей защищенной сети с сетями других предприятий.

20.6. Оператор АРМ - работник 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. Оператор не имеет полномочий для управления подсистемами обработки данных и СЗПДн.

20.6.1. 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.

20.7. Администратор корпоративной сети - работник Учреждения, ответственный за функционирование телекоммуникационной подсистемы ИСПДн. Администратор сети не имеет полномочий для управления подсистемами обработки данных и безопасности.

20.7.1. Администратор корпоративной сети обладает следующим уровнем доступа и знаний:

- обладает частью информации о системном и прикладном программном обеспечении ИСПДн;

- обладает полной информацией о технических средствах КС;

- имеет физический доступ к техническим средствам обработки информации и средствам защиты.

20.8. Технический специалист по обслуживанию - работник Учреждения, 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.

20.8.1. 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.

20.9. Программисты-разработчики – разработчики прикладного программного обеспечения, обеспечивающие его сопровождение на защищаемом объекте. К данной группе могут относиться как работники Учреждения, так и работники сторонних организаций.

20.9.1. Лицо этой категории:

- обладает информацией об алгоритмах и программах обработки информации на ИСПДн;

- обладает возможностями внесения ошибок, недекларированных возможностей, программных закладок, вредоносных программ в программное обеспечение ИСПДн на стадии ее разработки, внедрения и сопровождения;

- может располагать любыми фрагментами информации о топологии ИСПДн и технических средствах обработки и защиты ПДн, обрабатываемых в ИСПДн.

21. Требования к персоналу по обеспечению защиты ПДн

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

21.2. При вступлении в должность нового работника 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.

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

21.4. Работники Учреждения, 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.

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

21.6. Работники Учреждения 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.

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

21.8. Работникам запрещается разглашать защищаемую информацию, которая стала им известна при работе с информационными системами Учреждения, третьим лицам.

21.9. При работе с ПДн в ИСПДн работники Учреждения обязаны обеспечить отсутствие возможности просмотра ПДн третьими лицами с мониторов АРМ или терминалов.

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

21.11. Работники Учреждения 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 работников, которые нарушили принятые политику и процедуры безопасности ПДн.

21.12. Работники 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.

22. Должностные обязанности пользователей ИСПДн

22.1. Должностные обязанности пользователей ИСПДн описаны в следующих документах:

- Инструкция администратора ИСПДн;

- Инструкция администратора безопасности ИСПДн;

- Инструкция пользователя ИСПДн;

- Инструкция пользователя при возникновении внештатных ситуаций.

23. Ответственность работников ИСПДн Учреждения

23.1. 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.

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

23.3. Приведенные выше требования нормативных документов по защите информации должны быть отражены в должностных инструкциях работников Учреждения.