ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ ЗДРАВООХРАНЕНИЯ
РЕСПУБЛИКИ КАРЕЛИЯ

«РЕСПУБЛИКАНСКИЙ ПРОТИВОТУБЕРКУЛЕЗНЫЙ ДИСПАНСЕР»

«УТВЕРЖДАЮ»
Главный врач ГБУЗ «РПТД»
_____Ю.С. КОНОНЕНКО

«__» _____ 2018 г.

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

информационных систем персональных данных ГБУЗ «РПТД»

Петрозаводск
2018

СОДЕРЖАНИЕ

Оглавление

ОПРЕДЕЛЕНИЯ

В настоящем документе используются следующие термины и их определения:

Автоматизированная система – система, реализующая информационную технологию выполнения установленных функций с помощью персонала и комплекса средств автоматизации.

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

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

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

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

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

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

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

Вспомогательные технические средства и системы – технические средства и системы, не предназначенные для передачи, обработки и хранения персональных данных, устанавливаемые совместно с техническими средствами и системами, предназначенными для обработки персональных данных или в помещениях, в которых установлены информационные системы персональных данных.

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

Доступ к информации – возможность получения информации и ее использования.

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

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

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

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

Информационная система персональных данных (ИСПДн) – информационная система персональных данных - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических 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 (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Общедоступные персональные данные – персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

Оператор (персональных данных) – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку

персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

Технические средства информационной системы персональных данных – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки ПДн (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и 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 к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

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

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

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

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

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 на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

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

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

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

Учреждение – учреждения здравоохранения.

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(ые) рабочее(ие) место(а)

ВП – вредоносные программы

ВТСС – вспомогательные технические средства и системы

ИСПДн – информационная система персональных данных

КВС – корпоративная вычислительная сеть

КЗ – контролируемая зона

ЛВС – локальная вычислительная сеть

МЭ – межсетевой экран

НСД – несанкционированный доступ

ОС – операционная система

ПДн – персональные данные

ПК – персональные компьютеры

ПМВ – программно-математическое воздействие

ПО – программное обеспечение

ПЭМИН – побочные электромагнитные излучения и наводки РФ – Российская Федерация

САЗ – система анализа защищенности

СЗИ – средства защиты информации

СЗПДн – система (подсистема) защиты персональных данных

СОВ – система обнаружения вторжений

ТКУ И – технические каналы утечки информации УБПДн – угрозы безопасности персональных данных ЭВМ - электронная вычислительная машина

ВВЕДЕНИЕ

Политика информационной безопасности (далее – Политика) Государственного бюджетного учреждения здравоохранения Республики Карелия «Республиканский противотуберкулезный диспансер» (далее – Учреждение) определяет систему обеспечения информационной безопасности Учреждения.

Политика определяет основные цели и задачи, а также общую стратегию построения системы защиты персональных данных (СЗПДн) в Учреждении. Политика определяет основные требования и базовые подходы к их реализации для достижения требуемого уровня безопасности информации, а также требования к сотрудникам, являющимися пользователями ИСПДн в Учреждении, степень их ответственности, должностные обязанности сотрудников, ответственных за обеспечение безопасности ПДн в Учреждении.

Политика разработана в соответствии с системным подходом к обеспечению информационной безопасности. Системный подход предполагает проведение комплекса мероприятий, включающих исследование угроз информационной безопасности и разработку системы защиты ПДн с позиции комплексного применения технических и организационных мер и средств защиты.

Под информационной безопасностью ПДн понимается защищенность ПДн в обрабатывающей их инфраструктуре от любых случайных или злонамеренных воздействий, результатом которых может явиться нанесение ущерба самой информации, ее владельцам (субъектам ПДн) или инфраструктуре. Задачи информационной безопасности сводятся к минимизации ущерба от возможной реализации угроз безопасности ПДн, а также к прогнозированию и предотвращению таких воздействий.

Политика служит основой для разработки комплекса организационных и технических мер по обеспечению информационной безопасности Учреждения, а также организационных и распорядительных документов, обеспечивающих ее реализацию.

Политика является основой для:

- принятия управленческих решений и разработки практических мер по реализации политики и выработки комплекса согласованных мер нормативно-правового, технологического и организационно-технического характера, направленных на выявление, отражение и ликвидацию последствий реализации различных видов угроз ПДн;

- разработки предложений по совершенствованию правового, нормативного, методического, технического и организационного обеспечения безопасности ПДн в ИСПДн Учреждения.

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

- Федеральный закон от 27 июля 2006 года №149-ФЗ «Об информации, информационных технологиях и о защите информации»;

- Федеральный закон от 27 июля 2006 года №152-ФЗ «О персональных данных» (далее – Закон №152-ФЗ);

- постановление Правительства Российской Федерации от 21 марта 2012 года №211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»;

- постановление Правительства Российской Федерации от 1 ноября 2012 года №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

- приказ Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 года №21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

1. Общие положения

1.1. Безопасность ПДн достигается путем исключения несанкционированного, в том числе случайного, доступа к ПДн, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение ПДн, а также иных несанкционированных действий.

1.2. Информация и связанные с ней ресурсы должны быть доступны для авторизованных пользователей. Осуществляется своевременное обнаружение, реагирование на УБПДн, предотвращение преднамеренных или случайных, частичных или полных несанкционированных модификаций или уничтожения данных.

1.3. Состав объектов защиты представлен в Перечне ПДн, обрабатываемых в Учреждении.

2. Область действия

Выполнение положений настоящей Политики информационной безопасности является обязательным для всех сотрудников Учреждения.

3. Основные принципы обеспечения ИСПДн

3.1. Определенность целей. Функциональные цели и цели информационной безопасности информационных систем ПДн Учреждения должны быть явно определены. Неопределенность приводит к «расплывчатости», невозможности оценки адекватности принятых защитных мер.

3.2. Своевременность обнаружения проблем. Необходимо своевременно обнаруживать проблемы, потенциально способные повлиять на функциональные цели и цели информационной безопасности ИСПДн Учреждения.

3.3. Прогнозируемость развития проблем. Необходимо выявлять причинно-следственную связь возможных проблем и строить на этой основе точный прогноз их развития.

3.4. Оценка влияния проблем на функциональные цели. Необходимо адекватно оценивать степень влияния выявленных проблем на функциональные цели ИСПДн Учреждения.

3.5. Адекватность защитных мер. Необходимо выбирать защитные меры, адекватные моделям угроз и нарушителей, с учетом затрат на реализацию таких мер и объема возможных потерь от выполнения угроз.

3.6. Эффективность защитных мер. Необходимо эффективно реализовывать принятые защитные меры.

3.7. Использование опыта при принятии и реализации решений. Необходимо накапливать, обобщать и использовать как свой опыт, так и опыт других организаций на всех уровнях принятия решений и их исполнения.

3.8. Контролируемость защитных мер. Необходимо применять только те защитные меры, правильность работы которых может быть проверена, при этом необходимо регулярно оценивать адекватность защитных мер и эффективность их реализации с учетом влияния защитных мер на функциональные цели и цели информационной безопасности ИСПДн Учреждения.

4. Общие условия обработки ПДн

4.1. Обработка ПДн в Учреждения осуществляется в соответствии с принципами законности и справедливости.

4.2. Цели обработки ПДн:

– организация учета сотрудников Учяреждения для обеспечения соблюдения требований действующих нормативных правовых актов.

– представителей юридических лиц, заключивших с Учреждением договоры, является, заключение и исполнение Учреждения договора с юридическим лицом, и взаимодействие с представителями юридических лиц, связанное с исполнением заключенных Учреждением договоров.

– оказание медицинской помощи пациентам Учреждения.

4.3. Не допускается обработка ПДн, несовместимая с целями сбора ПДн.

4.4. Не допускается объединение баз данных, содержащих ПДн, обработка которых осуществляется в целях, несовместимых между собой.

4.5. Допускается обработка исключительно тех ПДн, которые отвечают целям их обработки.

4.6. Содержание и объем обрабатываемых ПДн должны соответствовать заявленным целям обработки.

4.7. Не допускается обработка ПДн, излишних по отношению к заявленным целям обработки.

4.8. При обработке ПДн должна быть обеспечена точность ПДн, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки ПДн.

4.9. Неполные или неточные данные должны быть удалены или уточнены.

4.10. Хранение ПДн должно осуществляться в форме, позволяющей

определить субъекта ПДн, не дольше, чем этого требуют цели обработки ПДн, если срок хранения ПДн не установлен законодательством.

4.11. По достижении целей обработки или в случае утраты необходимости в достижении этих целей, ПДн должны быть уничтожены или обезличены, если иное не предусмотрено законодательством.

4.12. Министерство при обработке ПДн обязано принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПДн, а также от иных неправомерных действий в отношении ПДн.

4.13. Обеспечение безопасности ПДн достигается, в частности:

– определением перечня угроз безопасности ПДн при их обработке в ИСПДн;

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

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

– оценкой эффективности принимаемых мер по обеспечению безопасности ПДн до ввода в эксплуатацию ИСПДн;

– учетом машинных носителей ПДн;

– обнаружением фактов несанкционированного доступа к ПДн и принятием мер;

– восстановлением ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

– установлением правил доступа к ПДн, обрабатываемым в ИСПДн, а также обеспечением регистрации и учета всех действий, совершаемых с ПДн в ИСПДн;

– контролем за принимаемыми мерами по обеспечению безопасности ПДн и уровня защищенности ИСПДн.

4.14. Перечень ПДн, обрабатываемых в ИСПДн Учреждения, утверждается приказом главного врача и по мере изменения состава обрабатываемых ПДн подлежит пересмотру и уточнению.

4.15. Субъектами ПДн, обработка которых осуществляется в ИСПДн Учреждения, являются:

- сотрудники Учреждения;
- пациенты Учреждения.

4.16. При определении объема и содержания обрабатываемых ПДн субъектов ПД Учреждения руководствуется вышеуказанными целями получения и обработки ПДн.

4.17. Доступ сотрудников Учреждения к ПДн, подлежащим обработке, разрешен только уполномоченным сотрудникам в соответствии со Списком лиц, допущенных к самостоятельной работе в ИСПДн. При этом указанным лицам предоставляется доступ только к ПДн, необходимым для выполнения их служебных обязанностей в пределах задач и функций их подразделений.

4.18. Порядок доступа субъекта ПДн к его персональным данным, обрабатываемым в ИСПДн Учреждения, осуществляется в соответствии с Законом №152-ФЗ «О персональных данных» и определяется Положением об обработке ПДн в Учреждения.

4.19. Перечень ИСПДн Учреждения утверждается приказом Министерства.

4.20. Организация и проведение мероприятий по обеспечению защиты ПДн в Учреждения осуществляется в соответствии с Положением по защите ПДн.

4.21. Общее руководство организацией работ по защите ПДн в Учреждении осуществляет ответственный за организацию обработки ПДн в Учреждении.

4.22. В целях обеспечения мероприятий, предусмотренных действующим законодательством Российской Федерации в области обработки ПДн, приказом главного врача Учреждения определен сотрудник, ответственный за:

– доведение до сведения сотрудников Учреждения положений законодательства Российской Федерации о ПДн, локальных актов Учреждения по вопросам обработки ПДн, требований к защите ПДн;

– осуществление внутреннего контроля за соблюдением Учреждения и сотрудниками Учреждения законодательства Российской Федерации о ПДн при обработке персональных данных в ИСПДн Учреждения, в том числе требований к защите ПДн, обрабатываемых в ИСПДн Учреждения.

4.23. Деятельность Учреждения по обеспечению безопасности ПДн контролируется уполномоченным органом по защите прав субъектов ПДн.

5. Система защиты ПДн

5.1. Уровень защищенности ПДн в ИСПДн Учреждения определяется:

- акте определения уровня защищенности ПДн при их обработке в ИСПДн;

- Модели угроз безопасности ПДн;

- нормативных документов ФСТЭК и ФСБ России.

5.2. На основании вышеуказанных документов определяется необходимый уровень защищенности ПД в ИСПДн Учреждения. По результатам анализа актуальных угроз безопасности ПДн, отраженных в Модели угроз безопасности ПДн, комиссией по защите информации Учреждения выносится заключение о необходимости использования технических средств и организационных мероприятий для обеспечения безопасности ПД.

6. Меры, методы и средства обеспечения требуемого уровня защищенности

6.1. Обеспечение требуемого уровня защищенности ПДн при их обработке в ИСПДн достигается с использованием мер, методов и средств безопасности. Все меры обеспечения безопасности ИСПДн Учреждения подразделяются на:

- законодательные (правовые);
- организационные (административные);
- физические;
- технические (аппаратные и программные).

6.2. Законодательные (правовые) меры защиты.

К законодательным (правовым) мерам защиты относятся действующие законы Российской Федерации, указы и нормативные акты, регламентирующие правила обращения с ПД, закрепляющие права и обязанности участников информационных отношений в процессе их обработки и использования, а также устанавливающие ответственность за нарушения этих правил, препятствуя тем самым неправомерному использованию ПД, и являющиеся сдерживающим фактором для потенциальных нарушителей.

Правовые меры защиты носят в основном упреждающий, профилактический характер и требуют постоянной разъяснительной работы с пользователями и обслуживающим персоналом ИСПДн.

6.3. Организационные (административные) меры защиты.

Организационные (административные) меры защиты – это меры организационного характера, регламентирующие процессы функционирования ИСПДн Учреждения, использование ресурсов ИСПДн, деятельность обслуживающего персонала, таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности или снизить размер потерь в случае их реализации.

Организационные меры:

- учет лиц, допущенных к работе с ПДн в ИСПДн Учреждения; лица, доступ которых к ПДн, обрабатываемым в информационной системе, необходим для выполнения служебных (трудовых) обязанностей, допускаются к соответствующим ПДн;

– для выбора и реализации методов и способов защиты информации в ИСПДн Учреждения требуется назначить структурное подразделение или должностное лицо (сотрудника), ответственное за обеспечение безопасности ПДн;

– обучение лиц, использующих средства защиты информации, применяемые в ИСПДн Учреждения, правилам работы с ними;

– разбирательство и составление заключений по фактам несоблюдения условий хранения носителей ПДн, использования средств защиты информации, которые могут привести к нарушению конфиденциальности ПДн или другим нарушениям, приводящим к снижению уровня защищенности ПДн, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений;

– размещение устройств вывода информации средств вычислительной техники, информационно-вычислительных комплексов, технических средств обработки графической, видео- и буквенно-цифровой информации, входящих в состав информационной системы, в помещениях, в которых они установлены, осуществляется таким образом, чтобы была исключена возможность просмотра посторонними лицами текстовой и графической видовой информации, содержащей ПД;

– соблюдение требований регламента процессов обслуживания и осуществления модификации аппаратных и программных ресурсов ИСПДн Учреждения;

– соблюдение требований регламента доступа в помещения с компонентами ИСПДн Учреждения;

– соблюдение требований инструкций ИСПДн Учрежения (администратора безопасности).

Главная цель административных мер – сформировать основные подходы к защите информации и обеспечить их выполнение, выделяя необходимые ресурсы и контролируя состояние дел.

Реализация подходов к защите ПД в ИСПДн Учреждения состоит из мер административного уровня и организационных (процедурных) мер защиты информации.

К административному уровню относятся решения руководства, затрагивающие деятельность ИСПДн в целом. Примером таких решений могут быть:

– принятие решения о формировании или пересмотре комплексной программы обеспечения безопасности ПД, определение ответственных за ее реализацию;

– формулирование целей, постановка задач, определение направлений деятельности в области безопасности ПД;

– принятие решений по вопросам реализации программы безопасности, которые рассматриваются в Учреждении;

– обеспечение нормативной (правовой) базы вопросов безопасности и т.п.

На организационном уровне определяются процедуры, правила достижения целей и решения задач информационной безопасности ПДн, достижение целей определяет:

– область применения политики безопасности ПДн;

– роли, обязанности и ответственность должностных лиц, отвечающих за проведение политики безопасности ПДн;

– права доступа к ПДн;

– использование мер и средства защиты;

– меры и средств обеспечения контроля за соблюдением введенного режима безопасности.

6.4. Физические меры защиты.

Физические меры защиты основаны на применении разного рода механических, электро- или электронно-механических устройств и сооружений, специально предназначенных для создания физических препятствий на возможных путях проникновения и доступа потенциальных нарушителей к компонентам системы и защищаемой информации, а также технических средств визуального наблюдения, связи и охранной сигнализации.

Физическая защита зданий, помещений, объектов и средств информатизации осуществляется путем установления соответствующих постов охраны, с помощью технических средств охраны или любыми другими способами, предотвращающими или существенно затрудняющими проникновение в здание, помещения посторонних лиц, хищение информационных носителей, самих средств информатизации, исключающими нахождение внутри контролируемой (охраняемой) зоны технических средств разведки.

6.5. Технические (аппаратно-программные) средства защиты.

Технические (аппаратно-программные) меры защиты основаны на использовании различных электронных устройств и специальных программ, входящих в состав ИСПДн и выполняющих (самостоятельно или в комплексе с другими средствами) функции защиты (идентификацию и аутентификацию пользователей, разграничение доступа к ресурсам, регистрацию событий, криптографическое закрытие информации и т.д.).

Успешное применение технических средств защиты предполагает, что выполнение перечисленных ниже требований обеспечено организационными (административными) мерами и используемыми физическими средствами защиты:

– обеспечена физическая целостность всех компонентов ИСПДн Учреждения;

– каждый сотрудник (пользователь ИСПДн) или группа пользователей имеет уникальное системное имя и минимально необходимые для выполнения им своих функциональных обязанностей полномочия по доступу к ресурсам системы;

– сетевое оборудование (концентраторы, коммутаторы, маршрутизаторы и т.п.) располагается в местах, недоступных для посторонних (специальных помещениях, шкафах, и т.п.);

– администратором безопасности совместно с ответственным за обеспечение безопасности ПДн осуществляется непрерывное управление и административная поддержка функционирования средств защиты.

7. Контроль эффективности системы защиты ИСПДн

Контроль эффективности системы защиты ИСПДн осуществляется Учреждением с периодичностью раз в полугодие. Целью контроля является своевременное выявление ненадлежащих режимов работы ИСПДн (отключение средств защиты, нарушение режимов защиты, несанкционированное изменение режима защиты и т.п.), а также прогнозирование и превентивное реагирование на новые угрозы безопасности ПДн.

Контроль может проводиться как администратором безопасности с помощью штатных средств системы защиты ПДн, так и с помощью специальных программных средств контроля, так и привлекаемыми для этой цели организациями, имеющими лицензию на этот вид деятельности, а также ФСТЭК России и ФСБ России в пределах их компетенции.

Оценка эффективности мер защиты ПДн проводится с использованием технических и программных средств контроля на предмет соответствия установленным действующим законодательством Российской Федерации требованиям.

8. Пользователи ИСПДн

Пользователи ИСПДн Учреждения, участвуют в обработке ПДн и являются:

- администратором безопасности (ИБ);

- оператором АРМ.

Администратор ИБ - сотрудник, ответственный за настройку, внедрение и сопровождение ИСПДн Учреждения, функционирование СЗПДн. Обеспечивает функционирование подсистемы управления доступом ИСПДн и уполномочен осуществлять предоставление конечного пользователя (оператора АРМ) к элементам, хранящим ПДн.

Администратор ИБ обладает следующим уровнем доступа и знаний:

- обладает полной информацией о системном и прикладном программном обеспечении ИСПДн Учреждения;

- обладает полной информацией о технических средствах и конфигурации ИСПДн Учреждения;

- имеет доступ ко всем техническим средствам обработки информации и данным ИСПДн Учреждения;

- обладает правами конфигурирования и административной настройки технических средств ИСПДн Учреждения;

- имеет доступ к средствам защиты информации и протоколирования и к части ключевых элементов ИСПДн Учреждения;

- имеет права доступа к конфигурированию технических средств сети;

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

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 Учреждения;

- осуществлять аудит средств защиты.

Оператор АРМ - пользователь, осуществляющий обработку ПДн в ИСПДн Учреждения. Оператор не имеет полномочий для управления подсистемами обработки данных и СЗПДн.

Оператор ИСПДн обладает следующим уровнем доступа и знаний:

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

- располагает конфиденциальными данными, к которым имеет доступ.

9. Требования к персоналу по обеспечению защиты ПДн

Все Пользователи ИСПДн Учреждения должны четко знать и строго выполнять установленные правила и обязанности по доступу к защищаемому объекту и соблюдению принятого режима безопасности ПДн.

Пользователи ИСПДн Учреждения должны быть ознакомлены со сведениями настоящей Политики, принятых процедур работы с элементами ИСПДн Учреждения и СЗПДн.

Пользователи ИСПДн Учреждения, использующие технические средства аутентификации, должны обеспечивать сохранность идентификаторов (электронных ключей) и не допускать несанкционированный доступ к ним, а так же возможность их утраты или использования третьими лицами. Пользователи несут персональную ответственность за сохранность идентификаторов.

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

Пользователи ИСПДн 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.

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

Пользователям запрещается разглашать защищаемую информацию, которая стала им известна при работе в ИСПДн Учреждения.

При работе с ПДн в ИСПДн Учреждения пользователи обязаны обеспечить отсутствие возможности просмотра ПД третьими лицами с мониторов АРМ.

Пользователи ИСПДн Учреждения обязаны без промедления сообщать обо всех наблюдаемых или подозрительных случаях работы системы, которые могут повлечь за собой угрозы безопасности ПДн, руководству подразделения и лицу, отвечающему за немедленное реагирование на угрозы безопасности ПДн.

10. Должностные обязанности пользователей ИСПДн

Должностные Обязанности пользователей ИСПДн Учреждения в следующих документах:

1. Инструкция администратора ЛВС;
2. Инструкция администратора безопасности ИСПДн;
3. Инструкция пользователя ИСПДн;
4. Инструкция администратора ИСПДн;
5. Инструкция пользователя при возникновении внештатных ситуаций.

11. Ответственность пользователей ИСПДн

В соответствии со ст.24 Законом №152-ФЗ лица, виновные в нарушении требований Закона №152-ФЗ, несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.

Действующее законодательство Российской Федерации позволяет предъявлять требования по обеспечению безопасной работы с защищаемой информацией и предусматривает ответственность за нарушение установленных

правил эксплуатации ЭВМ и систем, неправомерный доступ к информации, если эти действия привели к уничтожению, блокированию, модификации информации или нарушению работы ЭВМ или сетей (статьи 272, 273 и 274 Уголовного кодекса Российской Федерации).

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