Приложение к приказу
министерства здравоохранения
Рязанской области
от 17.09.2014 № 1467

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИСПДН МИНИСТЕРСТВА ЗДРАВООХРАНЕНИЯ РЯЗАНСКОЙ ОБЛАСТИ

Определения

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.

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.

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) – 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.

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

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.

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.

Оператор (персональных данных) – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующее и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

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 определённому или определяемому физическому лицу (субъекту персональных данных).

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

Программная закладка – код программы, преднамеренно внесенный в программу с целью осуществить утечку, изменить, блокировать, уничтожить информацию или уничтожить и модифицировать программное обеспечение информационной системы персональных данных и (или) блокировать аппаратные средства.

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

Распространение персональных данных – действия, направленные на раскрытие персональных данных неопределённому кругу лиц.

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.

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).

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

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

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

Обозначения и сокращения

ВП	вредоносная программа
ЗИР	защищаемый информационный ресурс
ИС	информационная система
ИСПДн	информационная система персональных данных
МЭ	межсетевой экран
НСД	несанкционированный доступ
ОС	операционная система
ПДн	персональные данные
ПМВ	программно-математические воздействия
ПО	программное обеспечение
СЗИ	средство защиты информации
СЗПДн	система защиты персональных данных
СКЗИ	средство криптографической защиты информации
БД	база данных
ТКУИ	технические каналы утечки информации
ТС	технические средства
УБПДн	угрозы безопасности персональных данных
ЭВМ	электронно-вычислительная машина

Введение

Настоящая Политика информационной безопасности (далее – Политика ИБ) разработана министерством здравоохранения Рязанской области и определяет основные цели и задачи, а также общую стратегию построения системы защиты персональных данных (СЗПДн) министерства здравоохранения Рязанской области. Политика определяет основные требования и базовые подходы к их реализации, для достижения требуемого уровня безопасности информации.

Политика разработана в соответствии с системным подходом к обеспечению информационной безопасности, который 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 персональных данных 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 министерства здравоохранения Рязанской области, а также нормативных и методических документов, обеспечивающих ее реализацию, и не предполагает подмены функций государственных органов власти Российской Федерации, отвечающих за обеспечение безопасности информационных технологий и защиту информации. Политика является методологической основой для:

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

− координации деятельности отделов министерства здравоохранения Рязанской области при проведении работ по развитию и эксплуатации информационных систем персональных данных с соблюдением требований обеспечения безопасности ПДн;

− разработки предложений по совершенствованию правового, нормативного, методического, технического и организационного обеспечения безопасности ПДн министерства здравоохранения Рязанской области.

Политика разработана на основании:

− Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;

– Типовых требований по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденных руководством 8 Центра ФСБ России 21.02.2008 г. № 149/6/6-662.

В Политике определены требования к персоналу, работающему в информационных системах персональных данных министерства здравоохранения Рязанской области степень ответственности персонала, структура и необходимый уровень защищенности, статус и должностные обязанности работников, ответственных за обеспечение безопасности персональных данных в ИСПДн.

1. Общие положения

1.1. Целью настоящей Политики является обеспечение безопасности персональных данных министерства здравоохранения Рязанской области от всех видов угроз, внешних и внутренних, умышленных и непреднамеренных, минимизация ущерба от возможной реализации угроз безопасности ПДн (УБПДн).

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. Персональные данные (ПДн) и связанные с ней ресурсы должны быть доступны для авторизованных пользователей. Должно осуществляться своевременное обнаружение и реагирование на угрозы безопасности персональных данных (далее – УБПДн).

2. Область действия

2.1. Требования настоящей Политики распространяются на всех работников министерства здравоохранения Рязанской области (штатных, временных, работающих по контракту и т.п.), а также всех прочих лиц (подрядчики, аудиторы и т.п.).

3. Система защиты персональных данных

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

- Отчёта по результатам обследования системы защиты персональных данных министерства здравоохранения Рязанской области (далее – Отчёт по результатам обследования);
- Перечня персональных данных, подлежащих защите;
- Акт определения уровня защищенности персональных данных, обрабатываемых в ИСПДн министерства здравоохранения Рязанской области;
- Модели угроз безопасности персональных данных, обрабатываемых в информационных системах персональных данных министерства здравоохранения Рязанской области (далее – Модель угроз);
- Частного технического задания на разработку системы защиты персональных данных министерства здравоохранения Рязанской области;
- Проекта системы защиты персональных данных информационных систем персональных данных министерства здравоохранения Рязанской области;
- Руководящих документов ФСТЭК и ФСБ России.

3.2. На основании этих документов определяется необходимый уровень защищенности ПДн ИСПДн министерства здравоохранения Рязанской области. На основании анализа актуальных угроз безопасности ПДн описанного в Отчете по результатам обследования и Модели угроз, делается заключение о необходимости использования технических средств и организационных мероприятий для обеспечения безопасности ПДн.

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

а) СЗИ от НСД:

- средства управления логическим доступом;
- средства регистрации и учета (самостоятельные или встроенные в другие СЗИ, обеспечивающие фиксацию важных с точки зрения обеспечения безопасности информации событий, происходящих в ИС);
- средства обеспечения целостности (самостоятельные или встроенные в другие СЗИ, обеспечивающие контроль целостности информационных ресурсов и программного обеспечения (далее – ПО);
- средства межсетевого взаимодействия;
- средства защиты от программно-математических воздействий (средства защиты от вредоносного ПО);
- средства защиты каналов связи;
- средства криптографической защиты информации (СКЗИ);
- средства инструментального анализа защищенности;
- средства обнаружения вторжений;

б) средства защиты от утечки конфиденциальной информации по техническим каналам:

- средства защиты от утечки видовой информации.

3.4. В список должны быть включены функции защиты, обеспечиваемые штатными средствами обработки ПДн, операционными системами (ОС),

прикладным ПО и специальными комплексами, реализующими средства защиты.

4. Основные принципы построения системы комплексной защиты информации

4.1. Построение системы обеспечения безопасности ПДн ИСПДн министерства здравоохранения Рязанской области и ее функционирование должны осуществляться в соответствии со следующими основными принципами:

- законность;
- системность;
- комплексность;
- непрерывность;
- своевременность;
- преемственность и непрерывность совершенствования;
- персональная ответственность;
- минимизация полномочий;
- взаимодействие и сотрудничество;
- гибкость системы защиты;
- простота применения средств защиты;
- научная обоснованность и техническая реализуемость;
- специализация и профессионализм;
- обязательность контроля.

4.1.1. Законность.

4.1.1.1. Данный принцип предполагает осуществление защитных мероприятий и разработку СЗПДн министерства здравоохранения Рязанской области в соответствии с действующим законодательством в области защиты ПДн и других нормативных актов по безопасности информации, утвержденных органами государственной власти и управления в пределах их компетенции. Работники и обслуживающий персонал ПДн ИСПДн министерства здравоохранения Рязанской области должны быть осведомлены о порядке работы с защищаемой информацией и об ответственности за защиту ПДн.

4.1.2. Системность.

4.1.2.1. Системный подход к построению СЗПДн министерства здравоохранения Рязанской области предполагает учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, существенно значимых для понимания и решения проблемы обеспечения безопасности ПДн ИСПДн министерства здравоохранения Рязанской области. При создании системы защиты должны учитываться все слабые и наиболее уязвимые места системы обработки ПДн, а также характер, возможные объекты и направления атак на систему со стороны нарушителей (особенно высококвалифицированных злоумышленников), пути проникновения в распределенные системы и НСД к информации. Система защиты должна

строиться с учетом не только всех известных каналов проникновения и НСД к информации, но и с учетом возможности появления принципиально новых путей реализации угроз безопасности.

4.1.3. Комплексность.

4.1.3.1. Комплексное использование методов и средств защиты предполагает согласованное применение разнородных средств при построении целостной системы защиты, перекрывающей все существенные (значимые) каналы реализации угроз и не содержащей слабых мест на стыках отдельных ее компонентов. Защита должна строиться эшелонировано. Для каждого канала утечки информации и для каждой угрозы безопасности должно существовать несколько защитных рубежей. Создание защитных рубежей осуществляется с учетом того, чтобы для их преодоления потенциальному злоумышленнику требовались профессиональные навыки в нескольких невзаимосвязанных областях.

4.1.4. Непрерывность защиты ПДн.

4.1.4.1. Защита ПДн – не разовое мероприятие и не простая совокупность проведенных мероприятий и установленных средств защиты, а непрерывный целенаправленный процесс, предполагающий принятие соответствующих мер на всех этапах жизненного цикла ИСПДн. ИСПДн должны находиться в защищенном состоянии на протяжении всего времени их функционирования. В соответствии с этим принципом должны приниматься меры по недопущению перехода ИСПДн в незащищенное состояние. Большинству физических и технических средств защиты для эффективного выполнения своих функций необходима постоянная техническая и организационная (административная) поддержка (своевременная смена и обеспечение правильного хранения и применения имен, паролей, ключей шифрования, переопределение полномочий и т.п.). Перерывы в работе средств защиты могут быть использованы злоумышленниками для анализа применяемых методов и средств защиты, для внедрения специальных программных и аппаратных «закладок» и других средств преодоления системы защиты после восстановления ее функционирования.

4.1.5. Своевременность.

4.1.5.1. Данный принцип предполагает упреждающий характер мер обеспечения безопасности ПДн, то есть постановку задач по комплексной защите ИСПДн и реализацию мер обеспечения безопасности ПДн на ранних стадиях разработки ИСПДн в целом, и ее системы защиты информации, в частности. Разработка системы защиты должна вестись параллельно с разработкой и развитием самой защищаемой системы. Это позволит учесть требования безопасности при проектировании архитектуры и, в конечном счете, создать более эффективные (как по затратам ресурсов, так и по стойкости) защищенные системы.

4.1.6. Преемственность и совершенствование.

4.1.6.1. Предполагают постоянное совершенствование мер и средств защиты информации на основе преемственности организационных и

технических решений, кадрового состава, анализа функционирования ИСПДн и ее системы защиты с учетом изменений в методах и средствах перехвата информации, нормативных требований по защите, достигнутого отечественного и зарубежного опыта в этой области.

4.1.7. Персональная ответственность.

4.1.7.1. Предполагает возложение ответственности за обеспечение безопасности ПДн и системы их обработки на каждого работника в пределах его полномочий. В соответствии с этим принципом распределение прав и обязанностей работников строится таким образом, чтобы в случае любого нарушения круг виновников был четко известен или сведен к минимуму.

4.1.8. Принцип минимизации полномочий.

4.1.8.1. Означает предоставление пользователям минимальных прав доступа в соответствии с производственной необходимостью, на основе принципа «все, что не разрешено, запрещено». Доступ к ПДн должен предоставляться только в том случае и объеме, если это необходимо работнику для выполнения его должностных обязанностей.

4.1.9. Взаимодействие и сотрудничество.

4.1.9.1. Предполагает создание благоприятной атмосферы в коллективах подразделений, обеспечивающих деятельность ИСПДн министерства здравоохранения Рязанской области, для снижения вероятности возникновения негативных действий связанных с человеческим фактором. В такой обстановке работники должны осознанно соблюдать установленные правила и оказывать содействие в деятельности ответственного за организацию обработки персональных данных и Администратора ИСПДн.

4.1.10. Гибкость системы защиты ПДн.

4.1.10.1. Принятые меры и установленные средства защиты, особенно в начальный период их эксплуатации, могут обеспечивать как чрезмерный, так и недостаточный уровень защиты. Для обеспечения возможности варьирования уровнем защищенности, средства защиты должны обладать определенной гибкостью. Особенно важным это свойство является в тех случаях, когда установку средств защиты необходимо осуществлять на работающую систему, не нарушая процесса ее нормального функционирования.

4.1.11. Простота применения средств защиты.

4.1.11.1. Механизмы защиты должны быть интуитивно понятны и просты в использовании. Применение средств защиты не должно быть связано со знанием специальных языков или с выполнением действий, требующих значительных дополнительных трудозатрат при обычной работе зарегистрированных установленным порядком пользователей, а также не должно требовать от пользователя выполнения рутинных малопонятных ему операций (ввод нескольких паролей и имен и т.д.). Должна достигаться автоматизация максимального числа действий пользователей и администраторов ИСПДн.

4.1.12. Научная обоснованность и техническая реализуемость.

4.1.12.1. Информационные технологии, технические и программные средства, средства и меры защиты информации должны быть реализованы на современном уровне развития науки и техники, научно обоснованы с точки зрения достижения заданного уровня безопасности информации и должны соответствовать установленным нормам и требованиям по безопасности ПДн. СЗПДн должна быть ориентирована на решения, возможные риски для которых и меры противодействия этим рискам прошли всестороннюю теоретическую и практическую проверку.

4.1.13. Специализация и профессионализм.

4.1.13.1. Предполагает привлечение к разработке средств и реализации мер защиты информации специализированных организаций, наиболее подготовленных к конкретному виду деятельности по обеспечению безопасности ПДн, имеющих опыт практической работы и государственную лицензию на право оказания услуг в этой области. Реализация административных мер и эксплуатация средств защиты должна осуществляться профессионально подготовленными специалистами министерства здравоохранения Рязанской области.

4.1.14. Обязательность контроля.

4.1.14.1. Предполагает обязательность и своевременность выявления и пресечения попыток нарушения установленных правил обеспечения безопасности ПДн на основе используемых систем и средств защиты информации при совершенствовании критериев и методов оценки эффективности этих систем и средств.

4.2. Контроль за деятельностью любого пользователя, каждого средства защиты и в отношении любого объекта защиты должен осуществляться на основе применения средств оперативного контроля и регистрации и должен охватывать как несанкционированные, так и санкционированные действия пользователей.

5. Требования к подсистемам СЗПДн

5.1. СЗПДн включает в себя следующие подсистемы:

- управления доступом,
- регистрации и учёта;
- обеспечения целостности;
- защиты от программно-математических воздействий;
- защиты каналов связи;
- межсетевого экранирования;
- обнаружения вторжений;
- криптографической защиты;
- инструментального анализа защищенности.

5.2. СЗПДн имеют различный функционал в зависимости от уровня защищенности ПДн, обрабатываемых в ИСПДн министерства здравоохранения Рязанской области.

5.2.1. Подсистема управления доступом.

5.2.1.1. Подсистема управления доступом предназначена для реализации следующих функций:

- Идентификация и проверка подлинности субъектов доступа при входе в систему по паролю условно-постоянного действия длинной не менее шести буквенно-цифровых символов.

5.2.1.2. 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.

5.2.2. Подсистема регистрации и учёта.

5.2.2.1. Подсистема регистрации и учёта предназначена для реализации следующих функций:

- Регистрация входа (выхода) субъектов доступа в систему (из системы), либо регистрация загрузки и инициализации операционной системы и ее программного останова. Регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения ИСПДн. В параметрах регистрации указываются дата и время входа (выхода) или загрузки (останова) системы, результат попытки входа (успешная или неуспешная), идентификатор (код или фамилия) субъекта, предъявленный при попытке доступа, код или пароль, предъявленный при неуспешной попытке.
- Учет всех защищаемых носителей информации с помощью их маркировки и занесением учетных данных в Журнал учета с отметкой об их выдаче (приеме).

5.2.3. Подсистема обеспечения целостности.

5.2.3.1. Подсистема целостности предназначена для реализации следующих функций:

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

- Периодическое тестирование функций системы защиты персональных данных при изменении программной среды и пользователей информационной системы с помощью тест – программ, имитирующих попытки несанкционированного доступа.
- Наличие средств восстановления системы защиты персональных данных, предусматривающие ведение двух копий программных компонентов средств защиты информации, их периодическое обновление и контроль работоспособности.

5.2.4. Подсистема защиты от программно-математических воздействий.

5.2.4.1. Подсистема защиты от программно-математических воздействий (подсистема антивирусной защиты) предназначена для реализации следующих функций:

- Автоматическая проверка на наличие вредоносных программ (далее – ВП) или последствий программно-математических воздействий (далее – ПМВ) при импорте в ИСПДн всех программных модулей (прикладных программ), которые могут содержать ВП, по их типовым шаблонам и с помощью эвристического анализа.
- Реализация механизмов автоматического блокирования обнаруженных ВП путем их удаления из программных модулей или уничтожения.
- Проверка на предмет наличия ВП в средствах защиты от ПМВ (при первом запуске средства защиты от ПМВ и с устанавливаемой периодичностью).
- Факт выявления ПМВ должен инициировать автоматическую проверку на предмет наличия ВП.
- Реализация механизма отката для устанавливаемого числа операций удаления ВП из оперативной или постоянной памяти, из программных модулей и прикладных программ или программных средств, содержащих ВП.
- На всех технических средствах ИСПДн должен проводиться непрерывный согласованный по единому сценарию автоматический мониторинг информационного обмена в ИСПДн с целью выявления проявлений ПМВ.
- Проверка целостности модулей средства защиты от ПМВ, необходимых для его корректного функционирования, при его загрузке с использованием контрольных сумм.
- Реализация механизмов проверки целостности пакетов обновлений средства защиты от ПМВ с использованием контрольных сумм.
- Восстановление средств защиты от ПМВ, предусматривающая ведение двух копий программных средств защиты, его периодическое обновление и контроль работоспособности.

5.2.5. Подсистема защиты каналов связи.

5.2.5.1. Подсистема защиты каналов связи предназначена для реализации следующих функций:

- Обмен персональными данными, при их обработке в информационной системе, по каналам связи, защита которых обеспечивается путем реализации

соответствующих организационных мер и (или) применения технических средств.

− Выделение канала связи, обеспечивающего защиту передаваемой информации.

− Аутентификация взаимодействующих информационных систем и проверка подлинности пользователей и целостности передаваемых данных.

− Предотвращение возможности отрицания пользователем факта отправки персональных данных другому пользователю.

− Предотвращение возможности отрицания пользователем факта получения персональных данных от другого пользователя.

5.2.6. Подсистема межсетевого экранирования.

5.2.6.1. Подсистема межсетевого экранирования предназначена для реализации следующих функций:

− Фильтрация на сетевом уровне для каждого сетевого пакета независимо (решение о фильтрации принимается на основе сетевых адресов отправителя и получателя или на основе других эквивалентных атрибутов).

− Фильтрация пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств.

− Идентификация и аутентификация администратора межсетевого экрана при его локальных запросах на доступ по идентификатору (коду) и паролю условно – постоянного действия.

− Регистрация входа (выхода) администратора межсетевого экрана в систему (из системы) либо загрузки и инициализации системы и ее программного останова (регистрация входа из системы не проводится в моменты аппаратурного отключения межсетевого экрана).

− Контроль целостности своей программной и информационной части.

− Восстановление свойств межсетевого экрана после сбоев и отказов оборудования.

− Регламентное тестирование реализации правил фильтрации, процесса идентификации и аутентификации администратора межсетевого экрана, процесса регистрации действий администратора межсетевого экрана, процесса контроля за целостностью программной и информационной части, процедуры восстановления.

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

5.2.7. Подсистема обнаружения вторжений.

5.2.7.1. Подсистема обнаружения вторжений предназначена для реализации следующих функций:

− Обнаружение вторжений должно обеспечиваться путем использования в составе ИСПДн программных или программно-аппаратных средств (систем) обнаружения вторжений, использующие сигнатурные методы анализа, а также методы выявления аномалий.

− Подсистема обнаружения вторжений проводится для информационной системы, подключённых к сетям международного информационного обмена,

путём использования в составе информационной системы программных или программно-аппаратных средств (систем) обнаружения вторжений.

5.2.8. Подсистема инструментального анализа защищенности.

5.2.8.1. Подсистема инструментального анализа защищённости предназначена для реализации следующих функций:

− Анализ защищенности проводится путем использования в составе ИСПДн программных или программно-аппаратных средств анализа защищенности.

− Для ИСПДн средствами анализа защищенности должна быть обеспечена возможность выявления уязвимостей, связанных с ошибками в конфигурации ПО ИСПДн, которые могут быть использованы нарушителем для реализации атаки на систему.

5.2.9. Подсистема криптографической защиты.

5.2.9.1. Подсистема криптографической защиты предназначена для реализации следующих функций:

− Приняты меры по исключению несанкционированного доступа в помещения, в которых размещены технические средства с установленным СКЗИ, посторонних лиц, по роду своей деятельности не являющихся персоналом, допущенным к работе в этих помещениях. В случае необходимости присутствия посторонних лиц в указанных помещениях обеспечен контроль за их действиями и обеспечена невозможность негативных действий с их стороны на СКЗИ, технические средства, на которых эксплуатируется СКЗИ и защищаемую информацию.

− Обеспечена невозможность доступа к ключевым носителям лиц, не назначенных для работы с конкретным ключевым носителем.

− Ключи на ключевых носителях, срок действия которых истек, уничтожаются путем переформатирования ключевых носителей средствами ПО СКЗИ, после чего ключевые носители могут использоваться для записи на них новой ключевой информации. Об уничтожении ключей делается соответствующая запись в Журнале.

6. Пользователи ИСПДн

6.1. В ИСПДн министерства здравоохранения Рязанской области можно выделить следующие группы пользователей, участвующих в обработке и хранении ПДн:

- Администратора ИСПДн;
- Ответственного за организацию обработки ПДн;
- Операторов (пользователей) обработки ИСПДн.

6.1.1. Администратор ИСПДн.

6.1.1.1. Администратор ИСПДн, работник министерства здравоохранения Рязанской области, ответственный за настройку, внедрение и сопровождение ИСПДн, обеспечивает функционирование ИСПДн и СЗПДн, включая обслуживание и настройку административной, серверной и клиентской

компонент, уполномочен осуществлять предоставление и разграничение доступа конечного пользователя (Оператора АРМ) к элементам хранящим персональные данные.

6.1.1.2. 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.
- 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)
- 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;
- уполномочен осуществлять аудит средств защиты;
- уполномочен устанавливать доверительные отношения своей защищенной сети с сетями других Учреждений.

6.1.2. Операторы (пользователи) обработки ИСПДн.

6.1.2.1. Оператор обработки ИСПДн, работник министерства здравоохранения Рязанской области, 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.

6.1.2.2. 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.

7. Требования к персоналу по обеспечению защиты ПДн

7.1. Все работники министерства здравоохранения Рязанской области, являющиеся пользователями ИСПДн, должны четко знать и строго выполнять установленные правила и обязанности по доступу к персональным данным и соблюдению режима безопасности ПДн.

7.2. При вступлении в должность нового работника ответственный за организацию обработки ПДн 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.

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

7.4. Работники министерства здравоохранения Рязанской области, использующие технические средства аутентификации, должны обеспечивать сохранность идентификаторов (электронных ключей) и не допускать несанкционированного к ним, а так же возможность их утери или использования третьими лицами. Пользователи несут персональную ответственность за сохранность идентификаторов.

7.5. Работники министерства здравоохранения Рязанской области должны следовать установленным процедурам поддержания режима безопасности ПДн при выборе и использовании паролей (если не используются технические средства аутентификации).

7.6. Работники министерства здравоохранения Рязанской области 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.

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

7.8. Работникам запрещается разглашать защищаемую информацию, которая стала им известна при работе с информационной системой министерства здравоохранения Рязанской области, третьим лицам.

7.9. При работе с ПДн в ИСПДн работники министерства здравоохранения Рязанской области обязаны обеспечить отсутствие возможности просмотра ПДн третьими лицами с мониторов АРМ или терминалов.

7.10. 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.

7.11. Работники министерства здравоохранения Рязанской области 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.

7.12. 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.

8. Должностные обязанности пользователей ИСПДн

8.1 Должностные обязанности пользователей ИСПДн описаны в следующих документах:

- Инструкция Администратора ИСПДн;
- Инструкция пользователя ИСПДн.

9. Ответственность пользователей ИСПДн

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

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

9.3. Администратор ИСПДн несет ответственность за все действия, совершенные от имени их учетных записей или системных учетных записей, если не доказан факт несанкционированного использования учетных записей.

9.4. При нарушениях работниками министерства здравоохранения Рязанской области – пользователей ИСПДн правил, связанных с безопасностью ПДн, они несут ответственность, установленную действующим законодательством Российской Федерации.