ФОНД КАПИТАЛЬНОГО РЕМОНТА МНОГОКВАРТИРНЫХ ДОМОВ РЯЗАНСКОЙ ОБЛАСТИ

390046, г. Рязань, ул. Маяковского, 1а, строение Е, e-mail: mail@fondkr62.ru, тел. 46-51-92

УТВЕРЖДАЮ

Генеральный директор
Фонда капитального ремонта
многоквартирных домов Рязанской
области

_____ М.В. Бондарева

09 января 2019 г.

Политика информационной безопасности информационных систем персональных данных Фонда капитального ремонта многоквартирных домов Рязанской области

Рязань
2019 г.

Содержание

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) разработана Фондом капитального ремонта многоквартирных домов Рязанской области и определяет основные цели и задачи, а также общую стратегию построения системы защиты персональных данных (СЗПДн) Фонда капитального ремонта многоквартирных домов 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 Фонда капитального ремонта многоквартирных домов 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 Фонда капитального ремонта многоквартирных домов 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 Фонда капитального ремонта многоквартирных домов Рязанской области.

Политика разработана на основании:

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

Приказа Федеральной службы безопасности Российской Федерации от 10 июля 2014 г. № 378 г. Москва «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности».

В Политике определены требования к персоналу, работающему в информационных системах персональных данных Фонда капитального ремонта многоквартирных домов 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 Фонда капитального ремонта многоквартирных домов 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 Фонда капитального ремонта многоквартирных домов 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 Фонда капитального ремонта многоквартирных домов Рязанской области (далее - Отчёт по результатам обследования);

Перечня персональных данных, подлежащих защите;

Акта определения уровня защищенности персональных данных, обрабатываемых в информационных системах персональных данных Фонда капитального ремонта многоквартирных домов Рязанской области;

Модели угроз безопасности персональных данных, обрабатываемых в информационных системах персональных данных Фонда капитального ремонта многоквартирных домов Рязанской области (далее - Модель угроз);

Частного технического задания на разработку системы защиты персональных данных Фонда капитального ремонта многоквартирных домов Рязанской области;

Проекта системы защиты персональных данных информационных систем персональных данных Фонда капитального ремонта многоквартирных домов Рязанской области;

Руководящих документов ФСТЭК и ФСБ России.

3.2 На основании этих документов определяется необходимый уровень защищенности ПДн ИСПДн Фонда капитального ремонта многоквартирных домов 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:

- идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ);
- управление доступом субъектов доступа к объектам доступа (УПД);

защита машинных носителей персональных данных (ЗНИ);

- регистрация событий безопасности (РСБ);
- антивирусная защита (АВЗ);

контроль (анализ) защищенности персональных данных (АНЗ);

- обеспечение доступности персональных данных (ОДТ);
- защита среды виртуализации (ЗСВ);

- защита технических средств (ЗТС);
- защита информационных систем, ее средств, систем связи и передачи данных (ЗИС);
- управление конфигурацией информационных систем и систем защиты персональных данных (УКФ).

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 Фонда капитального ремонта многоквартирных домов 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 Фонда капитального ремонта многоквартирных домов 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 Фонда капитального ремонта многоквартирных домов 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 Фонда капитального ремонта многоквартирных домов 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 Фонда капитального ремонта многоквартирных домов 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 Фонда капитального ремонта многоквартирных домов

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 Фонда капитального ремонта многоквартирных домов 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 организационные и технические меры защиты информации, реализуемые в информационных системах в рамках ее системы обеспечения информационной безопасности, в зависимости от угроз безопасности, используемых информационных технологий и структурно-функциональных характеристик автоматизированной системы должны обеспечивать:

- идентификацию и аутентификацию субъектов доступа и объектов доступа (ИАФ);
- управление доступом субъектов доступа к объектам доступа (УПД);
- ограничение программной среды (ОПС;)
- защиту машинных носителей информации (ЗНИ);
- регистрацию событий безопасности (РСБ);

- антивирусную защиту (АВЗ);
- обнаружение вторжений (СОВ);
- контроль (анализ) защищенности информации (АНЗ);
- обеспечение целостности информационных систем и информации (ОЦЛ);
- обеспечение доступности информации (ОДТ);
- защиту среды виртуализации (ЗСВ);
- защиту технических средств (ЗТС);
- защиту автоматизированной системы, ее средств, систем связи и передачи данных (ЗИС);
- управление конфигурацией информационных систем и системы защиты персональных данных (УКФ).

5.2 СЗПДн имеют различный функционал в зависимости от уровня защищенности ПДн, обрабатываемых в ИСПДн Организации.

5.2.1 Меры по идентификации и аутентификации субъектов доступа и объектов доступа должны обеспечивать присвоение субъектам и объектам доступа уникального признака (идентификатора), сравнение предъявляемого субъектом (объектом) доступа идентификатора с перечнем присвоенных идентификаторов, а также проверку принадлежности субъекту (объекту) доступа предъявленного им идентификатора (подтверждение подлинности).

5.2.2 Меры по управлению доступом субъектов доступа к объектам доступа должны обеспечивать управление правами и привилегиями субъектов доступа, разграничение доступа субъектов доступа к объектам доступа на основе совокупности установленных в информационных системах правил разграничения доступа, а также обеспечивать контроль соблюдения этих правил.

5.2.3 Меры по ограничению программной среды должны обеспечивать установку и (или) запуск только разрешенного к использованию в информационных системах программного обеспечения или исключать возможность установки и (или) запуска запрещенного к использованию в информационных системах программного обеспечения.

5.2.4 Меры по защите машинных носителей информации должны обеспечивать контроль доступа к машинным носителям информации и учет, контроль перемещения и использования.

5.2.5 Меры по регистрации событий безопасности должны обеспечивать сбор, запись, хранение и защиту информации о событиях безопасности в информационных системах, а также возможность просмотра и анализа информации о таких событиях и реагирование на них.

5.2.6 Меры по антивирусной защите должны обеспечивать обнаружение в информационных системах компьютерных программ либо иной компьютерной информации, предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирование на обнаружение этих программ и информации.

5.2.7 Меры по обнаружению (предотвращению) вторжений должны обеспечивать обнаружение действий в информационных системах, направленных на преднамеренный несанкционированный доступ к информации, специальные воздействия на информационные системы и (или) информацию в целях ее добывания, уничтожения, искажения и блокирования доступа к информации, а также реагирование на эти действия.

5.2.8 Меры по контролю (анализу) защищенности информации должны обеспечивать контроль уровня защищенности информации, содержащейся в информационных системах, путем проведения мероприятий по анализу защищенности информационных систем и тестированию системы защиты информации.

5.2.9 Меры по обеспечению целостности информационных систем и информации должны обеспечивать обнаружение фактов несанкционированного нарушения целостности

информационных систем и содержащейся в ней информации, а также возможность восстановления информационных систем и содержащейся в ней информации.

5.2.10 Меры по обеспечению доступности информации должны обеспечивать авторизованный доступ пользователей, имеющих права по такому доступу, к информации, содержащейся в информационных системах, в штатном режиме функционирования информационных систем.

5.2.11 Меры по защите среды виртуализации должны исключать несанкционированный доступ к информации, обрабатываемой в виртуальной инфраструктуре, и к компонентам виртуальной инфраструктуры, а также воздействие на информацию и компоненты, в том числе к средствам управления виртуальной инфраструктурой, монитору виртуальных машин (гипервизору), системе хранения данных (включая систему хранения образов виртуальной инфраструктуры), сети передачи данных через элементы виртуальной или физической инфраструктуры, гостевым операционным системам, виртуальным машинам (контейнерам), системе и сети репликации, терминальным и виртуальным устройствам.

5.2.12 Меры по защите технических средств должны исключать несанкционированный доступ к стационарным техническим средствам, обрабатывающим информацию, средствам, обеспечивающим функционирование информационных систем (далее - средства обеспечения функционирования), и в помещения, в которых они постоянно расположены, защиту технических средств от внешних воздействий, а также защиту информации, представленной в виде информативных электрических сигналов и физических полей.

5.2.13 Меры по защите информационных систем, их средств, систем связи и передачи данных должны обеспечивать защиту информации при взаимодействии информационных систем или их отдельных сегментов с иными информационными системами и информационнотелекоммуникационными сетями посредством применения архитектуры информационных систем, проектных решений по ее системе защиты информации, направленных на обеспечение защиты информации.

5.2.14 Меры по выявлению инцидентов и реагированию на них направлены на определение лиц, ответственных за выявление инцидентов и реагирование на них, обнаружение, идентификацию и регистрацию инцидентов, а также на своевременное информирование лиц о возникших инцидентах в информационных системах персональных данных.

Меры по управлению конфигурацией информационных систем и системы защиты персональных данных должны обеспечить управление изменениями конфигурации информационных систем, анализировать потенциальное воздействие планируемых изменений в конфигурации информационных систем и системы защиты персональных данных, а также определению лиц, которым разрешены действия по внесению изменений в конфигурацию информационных систем и системы защиты персональных данных.

6 Пользователи ИСПДн

6.1 В ИСПДн Фонда капитального ремонта многоквартирных домов 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 Фонда капитального ремонта многоквартирных домов 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 Фонда капитального ремонта многоквартирных домов 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 Фонда капитального ремонта многоквартирных домов 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 Фонда капитального ремонта многоквартирных домов 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 Фонда капитального ремонта многоквартирных домов Рязанской области должны следовать установленным процедурам поддержания режима безопасности ПДн

при выборе и использовании паролей (если не используются технические средства аутентификации).

7.6 Работники Фонда капитального ремонта многоквартирных домов Рязанской

области 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 информационными системами Фонда капитального ремонта многоквартирных домов Рязанской области, третьим лицам.

7.9 При работе с ПДн в ИСПДн работники Фонда капитального ремонта многоквартирных домов 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 Фонда капитального ремонта многоквартирных домов 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 Фонда капитального ремонта многоквартирных домов Рязанской области - пользователей ИСПДн правил, связанных с безопасностью ПДн. они несут ответственность, установленную действующим законодательством Российской Федерации.