Приложение № 5
к приказу от 15.05.2017 г. № 21

УТВЕРЖДАЮ

_____(В.В. Ионов)

«15» мая 2017 г.

ПОЛИТИКА
оператора в отношении обработки защищаемой информации,
в том числе персональных данных,
в Контрольно-счетной палате Рязанской области

г. Рязань
2017 г.

Содержание

Определения

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

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

Блокирование информации, в том числе персональных данных – временное прекращение обработки информации, в том числе персональных данных (за исключением случаев, если обработка необходима для уточнения информации).

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 защищаемую информацию или ресурсы информационной системы.

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.

Информационная система – совокупность содержащихся в базах данных информации, в том числе персональных данных, и обеспечивающих ее 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 информации, в том числе персональных данных – обязательное для соблюдения оператором или иным получившим доступ к информации (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 и (или) выходящей из информационной системы.

Нарушитель безопасности информации, в том числе персональных данных – физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности информации (персональных данных) при их обработке техническими средствами в информационных системах.

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

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 информации (персональных данных) – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с информацией (персональными данными), включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение информации (персональных данных).

Оператор (персональных данных) – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующее и (или) осуществляющие обработку информации (персональных данных), а также определяющие цели обработки информации (персональных данных), состав информации (персональных данных), подлежащих обработке, действия (операции), совершаемые с информацией (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 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 – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки информации (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 информации (персональных данных) – передача информации (персональных данных) на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

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

Уничтожение информации (персональных данных) – действия, в результате которых невозможно восстановить содержание информации (персональных данных) в информационной системе или в результате которых уничтожаются материальные носители информации (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
ГИС	– государственная информационная система
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 оператора в отношении обработки защищаемой информации, в том числе персональных данных (далее – Политика), разработана Контрольно-счетной палатой Рязанской области и определяет основные цели и задачи, а также общую стратегию построения системы защиты информации (СЗИ) Контрольно-счетной палаты Рязанской области. Политика определяет основные требования и базовые подходы к их реализации, для достижения требуемого уровня безопасности защищаемой информации, в том числе персональных данных (далее – ПДн).

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 информации, с позиции комплексного применения технических и организационных мер и средств защиты.

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

Политика служит основой для разработки комплекса организационных и технических мер по обеспечению информационной безопасности Контрольно-счетной палаты 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, в том числе ПДн. Политика является методологической основой для:

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

– координации деятельности работников при проведении работ по развитию и эксплуатации информационных систем с соблюдением требований обеспечения безопасности защищаемой информации;

– разработки предложений по совершенствованию правового, нормативного, методического, технического и организационного обеспечения безопасности защищаемой информации Контрольно-счетной палаты Рязанской области.

Политика разработана на основании:

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

– Приказа Федеральной службы безопасности РФ от 10.07.2014 г. № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»;

– Приказ Федеральной службы по техническому и экспортному контролю № 17 от 31 мая 2013 года «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

В Политике определены требования к персоналу, работающему в Контрольно-счетной палате Рязанской области, степень ответственности персонала, структура и необходимый уровень защищенности, статус и должностные обязанности работников, ответственных за обеспечение безопасности защищаемой информации, в том числе ПДн, в ИС.

1 Общие положения

Целью настоящей Политики является обеспечение безопасности защищаемой информации, в том числе ПДн, Контрольно-счетной палаты Рязанской области от всех видов угроз, внешних и внутренних, умышленных и непреднамеренных, минимизация ущерба от возможной реализации угроз безопасности информации (УБИ).

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

Защищаемая информация, в том числе ПДн, и связанные с ней ресурсы должны быть доступны для авторизованных пользователей. Должно осуществляться своевременное обнаружение и реагирование на угрозы безопасности защищаемой информации, в том числе ПДн.

2 Область действия

Требования настоящей Политики распространяются на всех работников Контрольно-счетной палаты Рязанской области (штатных, временных, работающих по контракту и т.п.), а также всех прочих лиц (подрядчики, аудиторы и т.п.).

3 Система защиты информации

3.1 Система защиты информации (СЗИ) строится на основании:

- Перечня защищаемой информации, в том числе ПДн, подлежащей защите;
- Акта классификации Контрольно-счетной палаты Рязанской области;
- Акта определения уровня защищенности информации, обрабатываемой в Контрольно-счетной палате Рязанской области;
- Модели угроз безопасности защищаемой информации, в том числе персональных данных, обрабатываемой в информационных системах Контрольно-счетной палаты Рязанской области (далее – Модель угроз);
- Частного технического задания на разработку системы защиты информации, в том числе персональных данных, Контрольно-счетной палаты Рязанской области (далее – Техническое задание);
- Проекта системы защиты информации, в том числе персональных данных, Контрольно-счетной палаты Рязанской области (далее – Проект);
- Руководящих документов ФСТЭК и ФСБ России.

3.2 На основании этих документов определяется необходимый уровень защищенности информации, обрабатываемой в Контрольно-счетной палате Рязанской области. На основании анализа актуальных угроз безопасности защищаемой информации, в том числе ПДн, описанного в Отчете по результатам обследования и Модели угроз, делается заключение о необходимости использования технических средств и организационных мероприятий для обеспечения безопасности защищаемой информации, в том числе ПДн.

3.3 В зависимости от уровня защищенности ИС и актуальных угроз, СЗИ может включать следующие технические средства:

- идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ);
- управление доступом субъектов доступа к объектам доступа (УПД);
- ограничение программной среды (ОПС;)
- защита машинных носителей информации (ЗНИ);
- регистрация событий безопасности (РСБ);
- антивирусная защита (АВЗ);
- обнаружение вторжений (СОВ);
- контроль (анализ) защищенности информации (АНЗ);
- обеспечение целостности информационной системы и информации (ОЦЛ);
- обеспечение доступности информации (ОДТ);
- защита среды виртуализации (ЗСВ);
- защита технических средств (ЗТС);
- защита автоматизированной системы, ее средств, систем связи и передачи данных (ЗИС).
- выявление инцидентов и реагирование на них (ИНЦ) (только для ИСПДн);
- управление конфигурацией информационной системы и системы защиты персональных данных (УКФ) (только для ИСПДн).

3.4 В список должны быть включены функции защиты, обеспечиваемые штатными средствами обработки информации, операционными системами (ОС), прикладным ПО и специальными комплексами, реализующими средства защиты.

4 Основные принципы построения системы комплексной защиты информации

Построение системы обеспечения безопасности информации Контрольно-счетной палаты 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.

Законность.

Данный принцип предполагает осуществление защитных мероприятий и разработку СЗИ Контрольно-счетной палаты Рязанской области в соответствии с действующим законодательством в области защиты информации и других нормативных актов по безопасности информации, утвержденных органами государственной власти и управления в пределах их компетенции. Работники и обслуживающий персонал защищаемой информации, в том числе ПДн, Контрольно-счетной палаты Рязанской области быть осведомлены о порядке работы с защищаемой информацией, в том числе ПДн, и об ответственности за ее защиту.

Системность.

Системный подход к построению СЗИ Контрольно-счетной палаты Рязанской области предполагает учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, существенно значимых для понимания и решения проблемы обеспечения безопасности информации Контрольно-счетной палаты Рязанской области. При создании системы защиты должны учитываться все слабые и наиболее уязвимые места системы обработки информации, 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.

Комплексность.

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.

Непрерывность защиты информации.

Защита информации, в том числе 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 ИС. ИС должны находиться в защищенном состоянии на протяжении всего времени их функционирования. В соответствии с этим принципом должны приниматься меры по недопущению перехода ИС 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.

Своевременность.

Данный принцип предполагает упреждающий характер мер обеспечения безопасности информации, то есть постановку задач по комплексной защите ИС и реализацию мер обеспечения безопасности информации на ранних стадиях разработки ИС 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.

Преемственность и совершенствование.

Предполагают постоянное совершенствование мер и средств защиты информации на основе преемственности организационных и технических решений, кадрового состава, анализа функционирования ИС 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.

Персональная ответственность.

Предполагает возложение ответственности за обеспечение безопасности информации 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.

Принцип минимизации полномочий.

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

Взаимодействие и сотрудничество.

Предполагает создание благоприятной атмосферы в коллективах подразделений, обеспечивающих деятельность Контрольно-счетной палаты 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 защищаемой информации, в том числе ПДн, и Администратора ИС.

Гибкость системы защиты информации.

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.

Простота применения средств защиты.

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 администратора ИС.

Научная обоснованность и техническая реализуемость.

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 информации. СЗИ должна быть ориентирована на решения, возможные риски для которых и меры противодействия этим рискам прошли всестороннюю теоретическую и практическую проверку.

Специализация и профессионализм.

Предполагает привлечение к разработке средств и реализации мер защиты информации специализированных организаций, наиболее подготовленных к конкретному виду деятельности по обеспечению безопасности информации, 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 Контрольно-счетной палаты Рязанской области.

Обязательность контроля.

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

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 СЗИ

СЗИ 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:

- идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ);
- управление доступом субъектов доступа к объектам доступа (УПД);
- ограничение программной среды (ОПС;)
- защита машинных носителей информации (ЗНИ);
- регистрация событий безопасности (РСБ);
- антивирусная защита (АВЗ);
- обнаружение вторжений (СОВ);
- контроль (анализ) защищенности информации (АНЗ);
- обеспечение целостности информационной системы и информации (ОЦЛ);
- обеспечение доступности информации (ОДТ);
- защита среды виртуализации (ЗСВ);
- защита технических средств (ЗТС);
- защита автоматизированной системы, ее средств, систем связи и передачи данных (ЗИС).
- выявление инцидентов и реагирование на них (ИНЦ) (только для ИСПДн);
- управление конфигурацией информационной системы и системы защиты персональных данных (УКФ) (только для ИСПДн).

СЗИ имеют различный функционал в зависимости от уровня защищенности информации, обрабатываемой в Контрольно-счетной палате Рязанской области.

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).

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 информационной системе правил разграничения доступа, а также обеспечивать контроль соблюдения этих правил.

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

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

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

Меры по антивирусной защите должны обеспечивать обнаружение в информационной системе 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.

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

Меры по контролю (анализу) защищенности информации должны обеспечивать контроль уровня защищенности информации, содержащейся в информационной системе, путем проведения мероприятий по анализу защищенности информационной системы и тестированию ее системы защиты информации.

Меры по обеспечению целостности информационной системы и информации должны обеспечивать обнаружение фактов несанкционированного нарушения целостности информационной системы и содержащейся в ней информации, а также возможность восстановления информационной системы и содержащейся в ней информации.

Меры по обеспечению доступности информации должны обеспечивать авторизованный доступ пользователей, имеющих права по такому доступу, к информации, содержащейся в информационной системе, в штатном режиме функционирования информационной системы.

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.

Меры по защите технических средств должны исключать несанкционированный доступ к стационарным техническим средствам, обрабатывающим информацию, средствам, обеспечивающим функционирование информационной системы (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.

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

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 информационной системы и системы защиты персональных данных должны обеспечить управление изменениями конфигурации информационной системы, анализировать потенциальное воздействие планируемых изменений в конфигурации информационной системы и системы защиты персональных данных, а также

определению лиц, которым разрешены действия по внесению изменений в конфигурацию информационной системы и системы защиты персональных данных.

6 Пользователи информационных систем Контрольно-счетной палаты Рязанской области

В Контрольно-счетной палате Рязанской области можно выделить следующие группы пользователей, участвующих в обработке и хранении защищаемой информации, в том числе персональных данных:

- Администратора ИБ;
- Администратора ИС;
- Ответственного за организацию обработки защищаемой информации, в том числе персональных данных;
- Операторов (пользователей) обработки ИС.

Администратор ИБ.

Администратор ИБ – работник Контрольно-счетной палаты Рязанской области, ответственный за функционирование СЗИ, включая обслуживание и настройку административной, серверной и клиентской компонент.

Администратор ИБ обладает следующим уровнем доступа и знаний:

- обладает правами Администратора;
- обладает полной информацией об ИС;
- имеет доступ к средствам защиты информации и протоколирования и к части ключевых элементов ИС;
- не имеет прав доступа к конфигурированию технических средств сети за исключением контрольных (инспекционных).

Администратор ИБ 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 ИС;
- осуществлять аудит средств защиты;
- устанавливать доверительные отношения своей защищенной сети с сетями других Учреждений.

Администратор ИС.

Администратор – работник Контрольно-счетной палаты Рязанской области, ответственный за настройку, внедрение и сопровождение ИС, обеспечивает функционирование подсистемы управления доступом ИС и уполномочен осуществлять предоставление и разграничение доступа конечного пользователя (Оператора АРМ) к элементам, хранящим защищаемую информацию, в том числе персональных данных.

Администратор ИС обладает следующим уровнем доступа и знаний:

- обладает полной информацией о системном и прикладном программном обеспечении ИС;
- обладает полной информацией о технических средствах и конфигурации ИС;
- имеет доступ ко всем техническим средствам обработки информации и данным ИС;
- обладает правами конфигурирования и административной настройки технических средств ИС.

Операторы (пользователи) обработки ИС.

Оператор обработки ИС, работник Контрольно-счетной палаты Рязанской области, осуществляющий обработку защищаемой информации. Обработка информации включает: возможность просмотра защищаемой информации, ручной ввод информации в систему ИС, формирование справок и отчетов по информации, полученной из ИС. Оператор не имеет полномочий для управления подсистемами обработки данных и СЗИ.

Оператор ИС обладает следующим уровнем доступа и знаний:

- обладает всеми необходимыми атрибутами (например, паролем), обеспечивающими доступ к некоторому подмножеству защищаемой информации;
- располагает конфиденциальными данными, к которым имеет доступ.

7 Требования к персоналу по обеспечению защиты информации, в том числе персональных данных

Все работники Контрольно-счетной палаты Рязанской области, являющиеся пользователями ИС, должны четко знать и строго выполнять установленные правила и обязанности по доступу к защищаемой информации и соблюдению режима безопасности информации.

При вступлении в должность нового работника ответственный за организацию обработки защищаемой информации, в том числе персональных данных, обязан организовать его ознакомление с должностной инструкцией и необходимыми документами, регламентирующими требования по защите информации, а также обучение навыкам выполнения процедур, необходимых для санкционированного использования ИС.

Работник должен быть ознакомлен со сведениями настоящей Политики, принятых процедур работы с элементами ИС и СЗИ.

Работники Контрольно-счетной палаты Рязанской области, использующие технические средства аутентификации, должны обеспечивать сохранность идентификаторов (электронных ключей) и не допускать несанкционированного доступа к ним, а также возможность их утери или использования третьими лицами. Пользователи несут персональную ответственность за сохранность идентификаторов.

Работники Контрольно-счетной палаты Рязанской области должны следовать установленным процедурам поддержания режима безопасности информации при выборе и использовании паролей (если не используются технические средства аутентификации).

Работники Контрольно-счетной палаты 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 информации и процедуры защиты оборудования, оставленного без присмотра, а также свои обязанности по обеспечению такой защиты.

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

Работникам запрещается разглашать защищаемую информацию, которая стала им известна при работе с информационными системами Контрольно-счетной палаты Рязанской области, третьим лицам.

При работе с защищаемой информацией, в том числе персональными данными, работники Контрольно-счетной палаты Рязанской области обязаны обеспечить отсутствие возможности просмотра защищаемой информации, в том числе персональных данных, третьими лицами с мониторов АРМ или терминалов.

При завершении работы с защищаемой информацией, в том числе персональными данными, 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.

Работники Контрольно-счетной палаты Рязанской области должны быть проинформированы об угрозах нарушения режима безопасности информации 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 защищаемой информации, в том числе ПДн.

Работники обязаны без промедления сообщать обо всех наблюдаемых или подозрительных случаях работы ИС, могущих повлечь за собой угрозы безопасности информации, а также о выявленных ими событиях, затрагивающих безопасность информации, руководству подразделения и лицу, отвечающему за немедленное реагирование на угрозы безопасности информации.

Должностные обязанности пользователей Контрольно-счетной палаты Рязанской области

Должностные обязанности пользователей информационных систем в Контрольно-счетной палате Рязанской области описаны в следующих документах:

- Инструкция Администратора ИБ;
- Инструкция Администратора ИС;
- Инструкция пользователя ИС.

8 Ответственность пользователей информационных систем Контрольно-счетной палаты Рязанской области

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

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

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

При нарушениях работниками Контрольно-счетной палаты Рязанской области – пользователей ИС Контрольно-счетной палаты Рязанской области правил, связанных с безопасностью информации, они несут ответственность, установленную действующим законодательством Российской Федерации.