Общество с ограниченной ответственностью

«Контур»

УТВЕРЖДЕНО
приказом
ООО «КОНТУР»
от 24.04.2024 №178-24

Экз. № 1

ПОЛИТИКА

ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ООО «КОНТУР»

Москва

2024

Содержание

1 Общие положения 3

2 Нормативные ссылки 3

3 Термины, определения, сокращения и обозначения 3

4 Описание объекта защиты 5

5 Цели и задачи по информационной безопасности 5

6 Модели угроз 7

7 Принципы обеспечения информационной безопасности 9

8 Зоны ответственности участников процесса обеспечения информационной безопасности 11

9 Основные требования по защите информации ограниченного доступа 13

10 Основные требования к процессам обеспечения информационной безопасности 16

11 Основные требования к процессам управления информационной безопасностью 20

12 Заключение 22

1 Общие положения

1.1 Настоящая Политика является документом, доступным всем сотрудникам ООО «Контур» и всем пользователям его ресурсов. Представляет собой официально принятую руководством ООО «Контур».

1.2 Основной задачей в области информационной безопасности ООО «Контур» признает совершенствование мер и средств обеспечения информационной безопасности информационных ресурсов ООО «Контур» в контексте развития законодательства и норм регулирования информационной деятельности.

1.3 Требования информационной безопасности, которые предъявляются ООО «Контур», соответствуют целям деятельности ООО «Контур» и предназначены для снижения рисков, связанных с информационной безопасностью, до приемлемого уровня.

1.4 Реализация и контроль исполнения требований, установленных настоящей Политикой, осуществляется работниками структурных подразделений ООО «Контур», ответственных за информационную безопасность, в соответствии со своими должностными инструкциями и другими внутренними документами ООО «Контур» по информационной безопасности.

2 Нормативные ссылки

Политика информационной безопасности в ООО «Контур» является важным документом, содержащим нормативные ссылки на законы, постановления и инструкции, утвержденные в Российской Федерации. Эти нормативные акты играют решающую роль в разработке и применении стратегий по обеспечению безопасности информации в организациях. Соблюдение указанных нормативных актов необходимо для обеспечения надежной защиты информации и защиты от угроз неправомерного использования данных.

3 Термины, определения, сокращения и обозначения

В данном документе используются следующие сокращения и соответствующие им обозначения:

АРМ	–	Автоматизированное рабочее место
БД	–	База данных
ГК РФ	–	Гражданский кодекс Российской Федерации
ИБ	–	Информационная безопасность
ИС	–	Информационная система
ИТ	–	Информационные технологии
ИСПД	–	Информационная система персональных данных
КоАП РФ	–	Кодекс об административных правонарушениях Российской Федерации
КРФ	–	Конституция Российской Федерации
НСД	–	Несанкционированный доступ;
ОРД	–	Организационно-распорядительная документация
ПД	–	Персональные данные
ПО	–	Программное обеспечение
МЭ	–	Межсетевой экран
КИ	–	Конфиденциальная информация
Положение	–	Положение «Информационной безопасности ООО «Контур»
Роскомнадзор	–	Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций Российской Федерации (уполномоченный орган по защите прав субъектов персональных данных)
РФ	–	Российская Федерация
СЗИ	–	Средства защиты информации
СКЗИ	–	Средства криптографической защиты информации

СЗПД	–	Система защиты персональных данных
ТЗ	–	Техническое задание
ТЗКИ	–	Техническая защита конфиденциальной информации
ТК РФ	–	Трудовой кодекс Российской Федерации
УЗ	–	Уровень защищенности [персональных данных при обработке в информационной системе персональных данных]
УК РФ	–	Уголовный кодекс Российской Федерации
ФСБ России	–	Федеральная служба безопасности Российской Федерации (федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности)
ФСТЭК России	–	Федеральная служба по техническому и экспортному контролю Российской Федерации (федеральный орган исполнительной власти, уполномоченный в области противодействия техническим разведкам и технической защиты информации)
149-ФЗ	–	Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»
152-ФЗ	–	Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»

3.2 В данном документе используются следующие термины и соответствующие им определения:

3.2.1 АРМ: Комплекс средств вычислительной техники и программного обеспечения, располагающийся, непосредственно на рабочем месте работника и предназначенный для автоматизации его работы в рамках специальности.

3.2.2 БД: Представленная в объективной форме совокупность самостоятельных материалов (статей, расчетов, нормативных актов, судебных решений и иных подобных материалов), систематизированных таким образом, чтобы эти материалы могли быть найдены и обработаны с помощью электронной вычислительной машины.

3.2.3 Информация: Сведения (сообщения, данные) независимо от формы их представления.

3.2.4 Информационная система: Совокупность содержащейся в БД информации и обеспечивающих ее обработку информационных технологий и технических средств.

3.2.5 Информационные технологии: Процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

3.2.6 Конфиденциальность информации: Обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

3.2.7 Материальный носитель информации: Материальный объект, используемый для закрепления и хранения на нем речевой, звуковой или изобразительной информации, в т.ч. в преобразованном виде.

3.2.8 Накопление информации: Действия, направленные на формирование исходного, несистематизированного массива ПД.

3.2.9 Неавтоматизированная обработка: Обработка информации без помощи средств вычислительной техники.

3.2.10 ПД: Любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту ПД).

3.2.11 Помещение: Часть объема здания или сооружения, имеющая определенное назначение и ограниченная строительными конструкциями, в которой: осуществляется обработка ПД; размещены используемые СКЗИ, хранятся СКЗИ и (или) носители ключевой, аутентифицирующей и парольной информации СКЗИ.

3.2.12 Программно-техническая база ИСПД: Программные и технические средства серверной части ИСПД, включая системное (в т.ч. операционная система), прикладное (в т.ч. система управления базами данных) и специальное программное обеспечение.

3.2.13 Сбор ПД: Целенаправленные действия оператора или специально привлеченных оператором для этого третьих лиц по получению ПД непосредственно от

субъекта ПД или его представителя.

3.2.14 СЗПД: Совокупность организационных и (или) технических мер, определенных с учетом актуальных угроз безопасности ПД и информационных технологий, используемых в ИСПД.

3.2.15 СКЗИ: Аппаратные, программные и программно-аппаратные шифровальные (криптографические) средства, реализующие алгоритмы криптографического преобразования информации для ограничения доступа к ней, в том числе при ее хранении, обработке и передаче.

3.2.16 Систематизация ПД: Действия, направленные на объединение и расположение ПД в определенной последовательности.

3.2.17 Техническое средство: Изделие, оборудование, аппаратура или их составные части, функционирование которых основано на законах электротехники, радиотехники и (или) электроники, содержащие электронные компоненты и (или) схемы, которые выполняют одну или несколько следующих функций: усиление, генерирование, преобразование, переключение и запоминание.

3.2.18 НКЦКИ: Национальный координационный центр по компьютерным инцидентам

3.2.19 ГосСОПКА: Государственная система обнаружения, предупреждения и ликвидации компьютерных атак

4 Описание объекта защиты

Основными объектами защиты системы ООО «Контур» являются:

– информационные ресурсы, содержащие коммерческую тайну, банковскую тайну, персональные данные физических лиц, сведения ограниченного распространения;

– информационные ресурсы, содержащие конфиденциальную информацию, включая персональные данные физических лиц, а также открыто распространяемая информация, необходимая для работы строительной компании, независимо от формы и вида ее представления;

– сотрудники строительной организации, являющиеся разработчиками и пользователями информационных систем;

– информационная инфраструктура, включающая системы обработки и анализа информации, технические и программные средства ее обработки, передачи и отображения, в том числе каналы информационного обмена и телекоммуникации, системы и средства защиты информации, объекты и помещения, в которых размещены такие системы.

5 Цели и задачи по информационной безопасности

5.1 Целями обеспечения информационной безопасности ООО «Контур» являются:

– защита интересов ООО «Контур», работников и иных субъектов информационных отношений, взаимодействующих с ООО «Контур», от возможного нанесения ущерба их деятельности посредством случайного или преднамеренного несанкционированного вмешательства в процесс функционирования информационных систем ООО «Контур», нарушения работы технических и программных средств, приводящего к недоступности информации, разглашению, искажению, уничтожению защищаемой информации и ее незаконному использованию;

– обеспечение устойчивого и корректного функционирования программных и аппаратных компонентов ООО «Контур» и предоставляемых сервисов;

– соблюдение правового режима использования программ обработки информации;

– предотвращение реализации угроз безопасности для деятельности ООО «Контур».

5.2 Объектами информационных правоотношений являются:

– информационные ресурсы, в том числе с ограниченным доступом;

– процессы обработки информации в информационных системах ООО «Контур», информационные технологии, регламенты и процедуры сбора, обработки, хранения и передачи информации;

– информационная инфраструктура, включающая системы обработки, хранения и анализа информации, технические и программные средства ее обработки, передачи и отображения, в том числе каналы информационного обмена и телекоммуникации;

– системы и средства защиты информации, объекты и помещения, в которых размещены хранилища информации.

5.3 Субъектами информационных отношений при использовании информационных систем ООО «Контур», заинтересованными в обеспечении информационной безопасности, являются:

– ООО «Контур», как собственник информационных ресурсов и оператор персональных данных;

– работники подразделений ООО «Контур», как пользователи и поставщики информации в информационные системы;

– юридические и физические лица, сведения о которых накапливаются, хранятся и обрабатываются в информационных системах ООО «Контур».

5.3 Субъекты информационных отношений заинтересованы в обеспечении:

– конфиденциальности определенной части информации;

– целостности информации;

– своевременного доступа к необходимой им информации;

– защиты от навязывания им ложной (недостоверной, искаженной) информации;

– разграничения ответственности за нарушения законных прав (интересов) других субъектов информационных отношений и установленных правил обращения с информацией;

– возможности осуществления непрерывного контроля и управления процессами обработки и передачи информации;

– защиты соответствующей части информации от незаконного ее тиражирования и распространения.

5.4 Для достижения целей защиты и обеспечения указанных свойств информации, система обеспечения информационной безопасности ООО «Контур» должна обеспечивать решение следующих задач:

5.4.1 Защиту от вмешательства в процесс функционирования информационных систем посторонних лиц (возможность использования системы и доступ к ее ресурсам должны иметь только зарегистрированные пользователи).

5.4.2 Разграничение доступа зарегистрированных пользователей к аппаратным, программным и информационным ресурсам информационных систем (возможность доступа только к тем ресурсам и выполнения только тех операций с ними, которые необходимы конкретным пользователям для выполнения своих служебных обязанностей).

5.4.3 Регистрацию и периодический контроль действий пользователей при использовании защищаемых ресурсов и периодический контроль корректности их действий.

5.4.4 Контроль целостности (обеспечение неизменности) среды исполнения программ и ее восстановление в случае нарушения.

5.4.5 Защиту от несанкционированной модификации и контроль целостности используемых в ООО «Контур» программных средств и данных, а также защиту от несанкционированного внедрения вредоносных программ.

5.4.6 Защиту информации ограниченного доступа, хранимой, обрабатываемой в ООО «Контур», от несанкционированного разглашения или искажения.

5.4.7 Обеспечение аутентификации пользователей, участвующих в информационном обмене (подтверждение подлинности отправителя и получателя информации), а также определение автора при создании и модификации информации.

5.4.8 Обеспечение исправности применяемых в информационных системах ООО «Контур» средств защиты информации.

5.4.9 Своевременное выявление источников угроз безопасности информации, причин и условий, способствующих нанесению ущерба заинтересованным субъектам информационных отношений, создание механизма оперативного реагирования на угрозы безопасности информации.

5.4.10 Создание условий для минимизации наносимого ущерба неправомерными действиями, ослабление негативного влияния и ликвидация последствий нарушения безопасности информации в ООО «Контур».

5.5 Решение вышеперечисленных задач в ООО «Контур» осуществляется:

5.5.1 Учетом всех подлежащих защите информационных ресурсов (каналов связи, аппаратных и программных средств).

5.5.2 Регламентацией процессов обработки подлежащей защите информации, действий работников ООО «Контур» и персонала, осуществляющего обслуживание и модификацию программных и технических средств, на основе утвержденных организационно-распорядительных документов по вопросам обеспечения информационной безопасности.

5.5.3 Назначением и подготовкой работников, ответственных за организацию и осуществление мероприятий по обеспечению информационной безопасности в ООО «Контур».

5.5.4 Наделением каждого работника минимально необходимыми для выполнения им своих функциональных обязанностей полномочиями по доступу к информационным ресурсам.

5.5.5 Знанием и строгим соблюдением всеми работниками, использующими и обслуживающими аппаратные и программные средства, требований организационно-распорядительных документов по вопросам обеспечения информационной безопасности.

5.5.6 Персональной ответственностью за свои действия каждого работника, участвующего в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющего доступ к ресурсам информационных систем.

5.5.7 Реализацией технологических процессов обработки информации с использованием комплексов организационно-технических мер защиты программного обеспечения, технических средств и данных.

5.5.8 Принятием мер по обеспечению физической целостности технических средств информационных систем и поддержанием необходимого уровня защищенности их компонентов.

5.5.9 Использованием физических и технических (программно-аппаратных) средств защиты ресурсов ООО «Контур» и административной поддержкой их использования.

5.5.10 Контролем соблюдения пользователями информационных систем требований по обеспечению информационной безопасности.

5.5.11 Юридической защитой интересов ООО «Контур» при взаимодействии с юридическими и физическими лицами от противоправных и несанкционированных действий со стороны этих лиц.

5.5.12 Проведением анализа эффективности принятых мер и применяемых средств защиты информации в ООО «Контур». Разработкой и реализацией предложений по совершенствованию СЗИ в ООО «Контур».

6 Модели угроз

Модели угроз и нарушителей являются один из основных разделов при развертывании, поддержании и совершенствовании системы обеспечения информационной безопасности. Уровень детализации параметров моделей угроз и нарушителей ИБ может варьироваться в зависимости от конкретных потребностей и определяется практическими требованиями. Модели угроз и нарушителей должны регулярного анализироваться и при необходимости пересматриваться.

Деятельность строительной компании поддерживается входящей в ее состав

информационной инфраструктурой, которая обеспечивает реализацию различных технологий и может быть представлена в виде иерархии следующих основных уровней:

- физического (линии связи, аппаратные средства и пр.);
- сетевого оборудования (маршрутизаторы, коммутаторы, концентраторы и пр.);
- сетевых приложений и сервисов;
- операционных систем (ОС);
- систем управления базами данных (СУБД);
- бизнес-процессов организации.

На каждом из уровней угрозы и их источники (в т.ч. злоумышленники), методы и средства защиты и подходы к оценке эффективности являются различными.

Основными источниками угроз ИБ являются:

- неблагоприятные события природного, техногенного и социального характера;
- зависимость от поставщиков/провайдеров/партнеров/клиентов;
- сбои, отказы, разрушения/повреждения программных и технических средств;
- работники, реализующие угрозы ИБ с использованием легально предоставленных им прав и полномочий (внутренние нарушители ИБ);
- работники, реализующие угрозы ИБ вне легально предоставленных им прав и полномочий, а также субъекты, не являющиеся работниками, но осуществляющие попытки НСД;
- несоответствие требованиям надзорных и регулирующих органов, действующему законодательству.

Наиболее актуальные источники угроз на физическом уровне, уровне сетевого оборудования и уровне сетевых приложений:

- внешние нарушители ИБ: лица, разрабатывающие/распространяющие вирусы и другие вредоносные программные коды; лица, организующие DoS, DDoS и иные виды атак; лица, осуществляющие попытки НСД;
- внутренние нарушители ИБ: персонал, имеющий права доступа к аппаратному оборудованию, в том числе сетевому, и т.п.;
- комбинированные источники угроз: внешние и внутренние нарушители ИБ, действующие совместно и (или) согласованно;
- сбои, отказы, разрушения/повреждения программных и технических средств.

Наиболее актуальные источники угроз на уровнях операционных систем, систем управления базами данных:

- комбинированные источники угроз: внешние и внутренние нарушители ИБ, действующие в сговоре.

Наиболее актуальные источники угроз на уровне бизнес-процессов:

- внутренние нарушители ИБ: авторизованные пользователи и операторы, представители менеджмента организации и пр.;
- комбинированные источники угроз: внешние нарушители ИБ (например, конкуренты) и внутренние, действующие в сговоре;
- несоответствие требованиям надзорных и регулирующих органов, действующему законодательству.

По отношению к строительной организации ООО «Контур» нарушители могут быть разделены на внешних и внутренних.

Внутренние нарушители

В качестве потенциальных внутренних нарушителей рассматриваются:

- сотрудники, не являющиеся зарегистрированными пользователями и не допущенные к ресурсам информационных систем, но имеющие доступ в здания и (или) помещения;

- персонал, обслуживающий технические средства информационной системы;
- сотрудники, обеспечивающие безопасность;
- руководители различных уровней.

Внешние нарушители

В качестве потенциальных внешних нарушителей рассматриваются:

- бывшие сотрудники;
- представители организаций, взаимодействующих по вопросам технического обеспечения;
- клиенты;
- конкурирующие организации;
- лица, случайно или умышленно проникшие в корпоративную информационную систему из внешних телекоммуникационных сетей (хакеры).

В отношении внутренних и внешних нарушителей принимаются следующие ограничения и предположения о характере их возможных действий:

- нарушитель скрывает свои несанкционированные действия от других сотрудников организации;
- несанкционированные действия нарушителя могут быть следствием ошибок пользователей, эксплуатирующего и обслуживающего персонала, а также недостатков принятой технологии обработки, хранения и передачи информации;
- в своей деятельности вероятный нарушитель может использовать любое имеющееся средство перехвата информации, воздействия на информацию и информационные системы, адекватные финансовые средства для подкупа персонала, шантаж, методы социальной инженерии и другие средства и методы для достижения стоящих перед ним целей;
- внешний нарушитель может действовать в сговоре с внутренним нарушителем.

7 Принципы обеспечения информационной безопасности

7.1 Принцип законности

7.1.1 При выборе защитных мероприятий, реализуемых системой обеспечения информационной безопасности, должно соблюдаться действующее законодательство.

7.1.2 Принятые меры защиты не должны препятствовать доступу к защищаемой информации со стороны государственных или правоохранительных органов, если такой доступ необходим в случаях, предусмотренных законодательством.

7.1.3 Программно-технические средства, применяемые в ООО «Контур», должны иметь соответствующие лицензии, официально приобретаться ООО «Контур» у представителей разработчиков этих средств.

7.2 Принцип системности

При построении системы обеспечения информационной безопасности необходимо применять системный подход, который предполагает взаимосвязь процессов организации защиты информационных ресурсов ООО «Контур», согласованное применение методов и средств защиты информационных ресурсов ООО «Контур».

7.3 Принцип координации

7.3.1 При организации действий по обеспечению информационной безопасности руководство ООО «Контур» обеспечивает четкую взаимосвязь соответствующих структурных подразделений между собой, с представителями сторонних организаций, оказывающих услуги в рамках договорных обязательств.

7.3.2 При построении, внедрении и эксплуатации системы обеспечения информационной безопасности руководство ООО «Контур» обеспечивает условия для

эффективной координации действий всех лиц, обеспечивающих информационную безопасность.

7.4 Принцип дружественности и простоты

7.4.1 Система обеспечения информационной безопасности в ООО «Контур» формируется таким образом, чтобы сделать максимально прозрачными для пользователей информационных систем ООО «Контур» процессы ее функционирования.

7.4.2 Система обеспечения информационной безопасности в ООО «Контур» выстраивается таким образом, чтобы ограничения организационного и технического характера, налагаемые на сотрудников ООО «Контур» в связи с реализацией защитных мер, существенно не затрудняли работу с ресурсами информационных систем ООО «Контур».

7.5 Принцип превентивности

Меры, применяемые ООО «Контур» с целью обеспечения информационной безопасности, должны носить упреждающий характер и не допускать реализацию соответствующих угроз и атак.

7.6 Принцип оптимальности и многоуровневости

7.6.1 Выбор единых программно-технических средств с целью сокращения расходов на создание и поддержку функционирования компонентов системы обеспечения информационной безопасности.

7.6.2 Применение разнородных программно-технических средств защиты, с целью построения целостной системы обеспечения информационной безопасности и устранения возможных уязвимостей.

7.6.3 Использование для создания разных рубежей обеспечения информационной безопасности средств, которые имеют схожие друг с другом функции, но разработанные различными производителями и имеющие различную логику построения защитных механизмов.

7.7 Принцип экономической целесообразности

7.7.1 Осуществление оценки уровня затрат на обеспечение безопасности, ценности информационных ресурсов и величины возможного ущерба для ООО «Контур» в случае нарушения конфиденциальности, целостности и доступности информационных ресурсов.

7.7.2 Выбор необходимого и достаточного уровня защиты информационных ресурсов, при котором затраты, риск и размер возможного ущерба являются приемлемыми.

7.8 Принцип непрерывности и недопустимости открытого состояния

7.8.1 Система обеспечения информационной безопасности в ООО «Контур» строится таким образом, чтобы процесс защиты информационных систем осуществлялся непрерывно и целенаправленно на протяжении всего жизненного цикла информационных систем.

7.8.2 Система обеспечения информационной безопасности при любых возникающих обстоятельствах либо полностью выполняет свои функции, либо полностью блокирует доступ.

7.9 Принцип профессионализма

7.9.1 Привлечение для разработки и внедрения системы обеспечения информационной безопасности, при необходимости, специализированных организаций, наиболее подготовленных к конкретному виду деятельности и имеющих соответствующие лицензии на выполнения работ и практический опыт в данной области.

7.9.2 Организация профессиональной подготовки своих работников для эксплуатации компонентов системы обеспечения информационной безопасности. Принцип выбора решений защиты.

7.9.3 Ориентация на применение современных высокотехнологичных решений и программно-технических средств защиты, хорошо зарекомендовавших себя, интуитивно понятных и не сложных в эксплуатации.

7.9.4 Использование оценки степени корректности функционирования и исполнения защитных функций, отказоустойчивости, проверки согласованности конфигурации различных компонентов и возможности осуществления централизованного администрирования при выборе решений по защите информационных систем.

7.10 Принцип развития

7.10.1 Развитие и обновление на регулярной основе существующей системы обеспечения информационной безопасности.

7.10.2 Ориентация на преемственность принятых ранее решений по защите, на анализ функционирования информационных систем и самой системы обеспечения информационной безопасности.

7.11 Принцип персональной ответственности и разделения обязанностей

7.11.1 Руководство ООО «Контур» определяет права и ответственность каждого конкретного работника (в пределах его должностных обязанностей) за обеспечение безопасности информационных ресурсов ООО «Контур».

7.11.2 Система обеспечения информационной безопасности ООО «Контур» обеспечивает разделение полномочий в информационных системах, обязанностей и ответственности между работниками, исключающее возможность нарушения критически важных для ООО «Контур» процессов или создания уязвимостей в защите информационных ресурсов.

7.12 Принцип минимизации привилегий пользователей

Обеспечение пользователей привилегиями минимально достаточными для выполнения ими своих функций в ООО «Контур», в соответствии со своими должностными обязанностями.

8 Зоны ответственности участников процесса обеспечения информационной безопасности

8.1 Руководство ООО «Контур»

8.1.1 Создает условия, при которых каждый работник ООО «Контур» знает свои обязанности и задачи в отношении информационных ресурсов и обеспечивает наличие необходимого разделения функций и полномочий в целях недопущения конфликта интересов.

8.1.2 Назначает работников, ответственных за создание и использование СЗИ, информации, обрабатываемой в ООО «Контур», реализацию процессов обеспечения информационной безопасности, а также их контроля.

8.1.3 Обеспечивает достаточную численность и квалификацию персонала, ответственного за построение и поддержание процессов обеспечения информационной безопасности, внедрение и управление СЗИ, а также контроль и мониторинг текущего состояния системы обеспечения информационной безопасности ООО «Контур».

8.1.4 Инициирует, осуществляет поддержку и контролирует выполнение всех процессов обеспечения информационной безопасности в ООО «Контур».

8.1.5 Анализирует результаты работ по обеспечению информационной безопасности и на их основе принимает решения о необходимости развития системы обеспечения информационной безопасности, ее развития, о возможности принятия остаточных рисков информационной безопасности, о выделении ресурсов, необходимых для реализации Политики информационной безопасности.

8.2 Компетентные подразделения ООО «Контур»

8.2.1 Организуют проведение необходимого инструктажа работников структурных подразделений в части вопросов безопасной эксплуатации информационных систем.

8.2.2 Обеспечивают защиту доступа ко всему серверному и коммутационному оборудованию, носителям информации, которые используются в соответствующих структурных подразделениях.

8.2.3 Осуществляют мероприятия по поддержке сопровождения и использования информационных систем.

8.2.4 Обеспечивают отказоустойчивость всего программно-аппаратного комплекса и процедуру регламентированного восстановления работоспособности после отказов компонентов.

8.2.5 Регулярно обновляют программные и программно-аппаратные комплексы СЗИ в ООО «Контур».

8.2.6 Осуществляют поддержку функционирования информационных систем и принимают необходимые меры по конфигурированию систем для обеспечения необходимого уровня информационной безопасности ООО «Контур».

8.2.7 Контролируют работоспособность устройств бесперебойного питания критичных для ООО «Контур» информационных систем.

8.2.8 Обеспечивают физическую защиту помещений, в которых располагаются критичные для ООО «Контур» информационные системы.

8.2.9 Обеспечивают сопровождение устройств контроля доступа в помещения ООО «Контур».

8.2.10 Обеспечивают защиту информационных ресурсов ООО «Контур» от случайного или намеренного уничтожения, искажения, разглашения.

8.2.11 Контролируют выполнение установленных правил и процедур обеспечения информационной безопасности в ООО «Контур».

8.3 Руководители структурных подразделений ООО «Контур»

8.3.1 Обязаны соблюдать требования действующего законодательства Российской Федерации и внутренних документов ООО «Контур» в части обеспечения информационной безопасности.

8.3.2 Обеспечивают контроль за соблюдением норм и правил обеспечения информационной безопасности в своем структурном подразделении и информируют компетентное подразделение о любых подозрительных событиях или нарушениях действующих правил обеспечения информационной безопасности.

8.3.3 Обеспечивают соответствие действий работников подразделения Политике информационной безопасности, внутренним документам по информационной безопасности и любым другим распоряжениям руководства ООО «Контур» по вопросам информационной безопасности.

8.3.4 Организуют проведение необходимого инструктажа по вопросам выполнения правил информационной безопасности для всех работников своего структурного подразделения.

8.3.5 Контролируют выполнение работниками в своем структурном подразделении установленных правил в целях обеспечения физической безопасности компьютерного оборудования и носителей информации.

8.3.6 Своевременно информируют руководство о всех выявленных сбоях в работе информационных систем.

8.3.7 Контролируют доступ к необходимым информационными ресурсам работников своего структурного подразделения в соответствии с потребностью в пределах служебных обязанностей.

8.4 Работники ООО «Контур»

8.4.1 Соблюдают и выполняют требования Политики информационной безопасности, соответствующих локальных актов, документов ООО «Контур» по вопросам информационной безопасности.

8.4.2 Соблюдают конфиденциальность данных, доступ к которым были ими получен.

8.4.3 Обеспечивают физическую безопасность всего технического оборудования и носителей информации, используемых в работе.

8.4.4 Не допускают самовольного подключения и использования в автоматизированной информационной системе личного компьютерного и цифрового оборудования, а также носителей информации.

8.4.5 Не допускают самовольную установку программного обеспечения на компьютеры, входящие в состав информационной системы.

8.4.6 Своевременно информируют руководителя своего структурного подразделения о всех случаях нарушения информационной безопасности и о всех выявленных сбоях в работе программных и программно-аппаратных средств.

8.4.7 Проявляют осмотрительность в отношении любых действий, которые могут повлечь за собой снижение уровня информационной безопасности.

8.5 Сторонние физические и юридические лица

Соблюдают и выполняют требования Политики информационной безопасности, соответствующих локальных актов и документов ООО «Контур» и других распоряжений руководства по вопросам информационной безопасности при исполнении договорных обязательств.

9 Основные требования по защите информации ограниченного доступа

9.1 Общие требования

9.1.1 В ООО «Контур» необходимо соблюдать режим безопасности, предусматривающий реализацию организационно-технических мероприятий, направленных на обеспечение конфиденциальности информации, доступ к которой ограничен в соответствии с требованиями законодательства Российской Федерации.

9.1.2 В ООО «Контур» должен быть разработан перечень информации ограниченного доступа.

9.1.3 Организация, как обладатель информации ограниченного доступа, при осуществлении своих прав обязано:

- соблюдать права и законные интересы иных лиц;
- принимать меры по защите информации;
- ограничивать доступ к информации, если такая обязанность установлена федеральными законами.

9.1.5 ООО «Контур», как обладатель информации ограниченного доступа, если иное не предусмотрено федеральными законами, вправе:

- разрешать или ограничивать доступ к информации, определять порядок и условия такого доступа;
- использовать информацию, в том числе распространять ее, по своему усмотрению;
- передавать информацию другим лицам на установленном законом основании;
- защищать установленными законом способами свои права в случае незаконного получения информации или ее незаконного использования иными лицами;
- осуществлять иные действия с информацией или разрешать осуществление таких действий, если эти действия не противоречат федеральным законам и другим нормативно-правовым актам регуляторов.

9.1.6 ООО «Контур», являясь обладателем информации ограниченного доступа, в случаях, установленных законодательством РФ, обязано обеспечить:

- предотвращение НСД к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;

– своевременное обнаружение фактов НСД к информации;

– недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;

– возможность регламентированного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;

– постоянный контроль за обеспечением уровня защищенности информации.

9.1.7 Защита информации ограниченного доступа представляет собой принятие правовых, организационных и технических мер, направленных на:

– соблюдение конфиденциальности информации (исключение неправомерного доступа, копирования, предоставления или распространения информации);

– обеспечение целостности информации (исключение неправомерного уничтожения или модифицирования информации);

– реализацию права на доступ к информации (исключение неправомерного блокирования информации).

9.2 Организация защиты конфиденциальной информации

9.2.1 При организации в ООО «Контур» защиты информации ограниченного доступа, необходимо руководствоваться требованиями Федерального закона от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации» и Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», которые регулируют отношения, связанные с установлением, изменением и прекращением режима обработки защищаемой информации. В ООО «Контур» необходимо соблюдать режим защиты конфиденциальной информации (далее – КИ):

– ограничение доступа к КИ, путем установления порядка обращения с этой информацией и контроля за соблюдением такого порядка;

– учет лиц, получивших доступ к КИ, и (или) лиц, которым такая информация была предоставлена или передана;

– регулирование отношений по использованию КИ, с работниками на основании трудовых договоров и контрагентами на основании гражданско-правовых договоров;

– использование материальных носителей, содержащих КИ в соответствии с утвержденным порядком, исключающим несанкционированный доступ к ним.

9.2.2 Для обеспечения защиты КИ, ООО «Контур» вправе применять средства и методы технической защиты, предпринимать другие, не противоречащие законодательству РФ, меры.

9.2.3 В целях охраны КИ, в рамках трудовых отношений необходимо:

– ознакомить под расписку работников, доступ которых к КИ, необходим для выполнения ими своих служебных обязанностей, с перечнем КИ, и установленным в ООО «Контур» режимом защиты КИ, а также мерами ответственности за его нарушение;

– создать работникам необходимые условия для соблюдения установленного режима защиты КИ.

9.2.4 Работники ООО «Контур», обязаны выполнять установленный в ООО «Контур» режим защиты КИ, не разглашать информацию, составляющую КИ, и не использовать эту информацию в личных целях.

9.3 Особенности защиты персональных данных

9.3.1 При организации в ООО «Контур» защиты персональных данных необходимо руководствоваться требованиями Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных», который регулирует отношения, связанные с обработкой и хранением персональных данных граждан, и определяет требования по защите их конфиденциальности.

9.3.2 ООО «Контур» самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей,

предусмотренных Федеральным законом №152-ФЗ и принятыми в соответствии с ним нормативными правовыми актами, если иное не предусмотрено Федеральным законом №152-ФЗ или другими федеральными законами.

9.3.3 Перечень мер, выполнение которых обеспечивает ООО «Контур» в качестве оператора персональных данных, должен включать:

– назначение в ООО «Контур» ответственного за организацию обработки персональных данных;

– издание ООО «Контур» документов, определяющих его политику в отношении обработки персональных данных, локальных актов по вопросам обработки персональных данных, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства РФ, устранение последствий таких нарушений;

– применение правовых, организационных и технических мер по обеспечению безопасности персональных данных в соответствии со статьей 19 Федерального закона

№152-ФЗ;

– оценку вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона №152-ФЗ, соотношение указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом №152-ФЗ;

– ознакомление работников ООО «Контур», непосредственно осуществляющих обработку персональных данных, с положениями законодательства РФ о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику ООО «Контур» в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных и обучение, при необходимости, указанных работников.

9.3.4 ООО «Контур» при обработке персональных данных обязано принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

9.3.5 Обеспечение безопасности персональных данных достигается, в частности:

– определением угроз и нарушителей безопасности персональных данных при их обработке в информационных системах персональных данных;

– проведением классификации ИСПДн в соответствии с требованиями Постановления Правительства РФ от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», и определение класса защищенности для ИСПДн;

– применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в ИСПДн, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает выбранные уровни защищенности персональных данных;

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

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

– учетом машинных носителей персональных данных;

– обнаружением фактов НСД к персональным данным и принятием мер; восстановлением персональных данных, модифицированных или уничтоженных вследствие НСД к ним;

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

– контролем за принимаемыми мерами по обеспечению безопасности

персональных данных и уровня защищенности ИСПДн.

9.3.6 Работники ООО «Контур» должны быть ознакомлены под роспись с документами ООО «Контур», устанавливающими порядок обработки персональных данных, а также об их правах, обязанностях и ответственности.

10 Основные требования к процессам обеспечения информационной безопасности

10.1 Общие положения

Методическое руководство, разработку конкретных требований по защите информации, согласование выбора средств вычислительной техники и связи, технических и программных средств защиты, организацию работ по выявлению возможностей и предупреждению утечки и нарушения целостности защищаемой информации осуществляют компетентные подразделения ООО «Контур».

10.2 Физическая безопасность и безопасность на рабочем месте

10.2.1 Система защиты зданий и помещений ООО «Контур», объектов и технических средств информационных систем ООО «Контур» обеспечивает выполнение следующих функций:

- разграничение доступа работников в помещения ООО «Контур» в соответствии с их полномочиями и функциональными обязанностями;
- регистрацию фактов входа работников в помещения с повышенными
- требованиями к режиму их посещения (серверные помещения, архивы и т.д.);
- регистрацию фактов входа посторонних лиц в здания ООО «Контур»;
- предотвращение доступа посторонних лиц в помещения, где размещены аппаратные и сетевые ресурсы информационных систем;
- разрешительный режим вноса/выноса (ввоза/вывоза) компьютерного оборудования, средств записи и хранения информации.

10.2.2 Определяется перечень технических средств, находящихся в специальных контролируемых зонах.

10.2.3 К техническим средствам, которые выделяются в специальные контролируемые зоны необходимо отнести следующие группы ресурсов:

- основные информационные серверы и средства вычислительной техники, на которых осуществляется обработка и хранение информации ограниченного распространения;
- сетевое оборудование и серверы, обеспечивающие работу критических систем;
- файловые серверы, на которых хранятся данные, в том числе резервные;
- критичные для деятельности ООО «Контур» системы и коммуникационное оборудование, обеспечивающее внешние коммуникации ООО «Контур».

10.2.4 Контролируемые зоны защищаются соответствующими системами контроля и управления доступом, обеспечивая доступ только авторизованному персоналу.

10.2.5 Размещение и эксплуатация рабочих станций, серверов и сетевого оборудования ООО «Контур» осуществляется в помещениях, оборудованных замками, средствами сигнализации и (при необходимости) постоянно находящихся под охраной или наблюдением. Размещение технических средств вывода и отображения информации в помещениях ООО «Контур» производится с учетом исключения возможности визуального просмотра информации посторонними лицами и персоналом, не допущенным к работе с данной информацией.

10.2.6 Работники ООО «Контур» на момент своего отсутствия на рабочем месте обязаны исключить возможность наличия на рабочем столе документов или носителей с защищаемой информацией.

10.2.7 Технические средства и оборудование должны размещаться и храниться таким образом, чтобы сократить возможный риск его повреждения и угрозы несанкционированного доступа.

10.2.8 Помещения ООО «Контур» должны быть оборудованы детекторами огня и дыма, огнетушителями, системами кондиционирования воздуха, средствами охранно-пожарной сигнализации.

10.2.9 Основное техническое оборудование ООО «Контур» должно быть защищено от перебоев в подаче электроэнергии путем подключения к электросети с применением источников бесперебойного питания. Источники бесперебойного питания необходимо регулярно тестировать и проверять уполномоченным работникам ООО «Контур» в соответствии с рекомендациями производителя.

10.2.10 Пользователи портативных технических средств не должны оставлять техническое оборудование и носители информации без присмотра.

10.2.11 Портативные технические средства не должны оставаться за пределами контролируемой зоны ООО «Контур» дольше, чем того требует служебная необходимость, если иное не определено руководством ООО «Контур».

10.3 Безопасность при работе с носителями информации

10.3.1 В ООО «Контур» должны соблюдаться меры по безопасной работе с электронными носителями информации с целью контроля их использования, для предотвращения несанкционированного копирования и разглашения защищаемой информации, внесения изменений или уничтожения указанной информации, а также внесения изменений в работу информационных систем.

10.3.1 Работники ООО «Контур» должны использовать электронные носители информации только для выполнения своих служебных обязанностей. Использование электронных носителей информации в ООО «Контур» в иных целях строго запрещено.

10.3.2 Электронные носители информации в ООО «Контур» должны быть учтены путем присвоения каждому носителю инвентаризационного номера и назначения владельца.

10.3.3 Электронные носители информации должны храниться в помещениях, исключающих получение к ним НСД, при этом должен быть обеспечен контроль доступа к носителям.

10.3.4 Для контроля процессов использования и хранения электронных носителей информации должен быть разработан порядок плановой инвентаризации носителей.

10.3.5 В случае кражи или потери электронных носителей информации, а также иных инцидентов, которые могут привести к разглашению защищаемой информации, должны проводиться мероприятия по расследованию указанных инцидентов.

10.2.12 При снятии электронного носителя информации с эксплуатации, все данные, хранящиеся на нем, должны быть гарантированно стерты.

10.2.13 При утилизации электронных носителей информации должна быть обеспечена невозможность восстановления записанной на них информации.

10.2.14 Факт уничтожения информации и утилизации носителя информации фиксируется в соответствии с порядком, установленным в ООО «Контур».

10.4 Техническое обслуживание оборудования

10.4.1 Технические средства всех систем ООО «Контур» должны проходить на регулярной основе сервисное обслуживание в соответствии с рекомендациями производителей оборудования.

10.4.2 Ремонт и сервисное обслуживание оборудования должны выполняться только квалифицированным персоналом.

10.4.3 Техническое обслуживание оборудования и систем сторонними организациями не должно приводить к риску нарушения конфиденциальности защищаемой информации.

10.5 Взаимодействие с третьими лицами

В целях обеспечения информационной безопасности ООО «Контур» при взаимодействии с третьими лицами должны выполняться следующие мероприятия:

- заключение соглашения о неразглашении конфиденциальной информации;
- контроль за действиями третьих лиц;
- в договорах с третьими лицами предусматривать право ООО «Контур» на проведение аудита обеспечения безопасности той информации, которая передается третьим лицам.

10.6 Управление жизненным циклом информационных систем

10.6.1 Мероприятия по управлению жизненным циклом автоматизированных информационных систем должны быть направлены на обеспечение информационной безопасности при вводе в действие, эксплуатации, сопровождении и модернизации, вывода из эксплуатации информационных систем, автоматизирующих деятельность ООО «Контур».

10.6.2 Основой при выборе или разработке информационных систем должны являться технические задания, содержащие требования информационной безопасности для информационных систем.

10.6.3 Любое планируемое к внедрению изменение информационной системы предварительно должно быть протестировано на совместимость и отсутствие нарушений работоспособности системных компонентов.

10.6.4 Работы по модернизации автоматизированной информационной системы, в том числе по установке программного обеспечения и обновлений, должны проводиться в нерабочее время или время наименьшей рабочей нагрузки.

10.6.5 При выводе из эксплуатации автоматизированных информационных систем должно обеспечиваться гарантированное удаление обрабатываемой и хранимой в них информации с использованием специализированных программных средств или путем физического уничтожения носителей информации.

10.6.6 Все процедуры обеспечения информационной безопасности, установленные в ООО «Контур» в отношении информационных систем, должны выполняться и контролироваться ответственными за информационную безопасность лицами.

10.7 Антивирусная защита

10.7.1 В целях предупреждения, обнаружения и устранения вредоносных программ в ООО «Контур» на постоянной основе должны использоваться средства антивирусной защиты.

10.7.2 Обязательному антивирусному контролю должна подлежать любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая по телекоммуникационным каналам, а также информация, хранимая на подключаемых съемных носителях, при непосредственном обращении к ней.

10.7.3 При установке программного обеспечения на серверы информационных систем ООО «Контур» или их обновлении должна автоматически выполняться предварительная проверка данного программного обеспечения на отсутствие вредоносного программного обеспечения.

10.7.4 Сигнатурные базы вредоносного программного обеспечения и антивирусные средства защиты должны регулярно обновляться.

10.7.5 Пользователи информационных систем ООО «Контур» не должны иметь возможность получения доступа к конфигурации антивирусного средства защиты или его отключения.

10.7.6 В ООО «Контур» необходимо определить процедуру для обработки и восстановления инфицированных данных и отслеживание источника заражения.

10.8 Контроль доступа к информационным системам

10.8.1 Все работники ООО «Контур», допущенные к работе с информационными системами, несут персональную ответственность за нарушения установленного порядка

обработки информации, правил хранения, использования и передачи, находящихся в их распоряжении защищаемых ресурсов системы.

10.8.2 Уровень полномочий пользователя в информационной системе ООО «Контур» должен определяться в соответствии с его должностными обязанностями и производственной необходимостью.

10.8.3 Доступ пользователей к информационным системам ООО «Контур» должен контролироваться администратором системы.

10.8.4 Осуществление регулярного контроля выполнения политик и иных документов, касающихся регламентации допуска работников ООО «Контур» к информационным системам.

10.9 Идентификация и аутентификация

10.9.1 Доступ пользователей к информационным системам должен предоставляться только после успешного завершения процедур идентификации, аутентификации и авторизации.

10.9.2 Получение пользователем имени в системе и парольной информации, которые обеспечивают доступ пользователя к ресурсам системы, должно осуществляться по представлению руководителей структурных подразделений.

10.10 Безопасность пароля

10.10.1 С целью обеспечения защиты от несанкционированного доступа к информационным системам устанавливаются требования к выбору парольной информации, обеспечивающие достаточную степень стойкости паролей.

10.10.2 Для обеспечения конфиденциальности парольной информации пользователю запрещается хранить значения своих паролей на бумажном носителе в открытом виде и в свободном доступе.

10.10.3 Для обеспечения конфиденциальности парольной информации пользователям запрещается передавать значения своих паролей третьим лицам.

10.10.4 При вводе пароля пользователем для доступа к информационной системе ООО «Контур» должно исключаться отображение парольной информации на экране монитора в открытом виде.

10.10.5 Процедура смены парольной информации в информационных системах ООО «Контур» должна проводиться на регулярной основе.

10.11 Регистрация событий

Осуществление регистрации событий безопасности на всех компонентах информационных систем ООО «Контур», в которых обрабатывается, хранится или по средствам которых передается защищаемая информация.

10.12 Использование СКЗИ

10.12.1 Решение об использовании СКЗИ в интересах защиты собственных информационных ресурсов принимается руководством ООО «Контур» в соответствии с законодательством Российской Федерации.

10.12.2 При эксплуатации СКЗИ и ключевой информации все сотрудники ООО «Контур» должны выполнять требования нормативных правовых актов, издаваемых федеральным органом исполнительной власти в области обеспечения безопасности, документов ООО «Контур» по обеспечению безопасности использования СКЗИ, а также эксплуатационной документации производителя СКЗИ.

10.13 Безопасность информационной сети

10.13.1 Установление надлежащего контроля в отношении локальной вычислительной сети и всех внешних информационных коммуникаций ООО «Контур» для обеспечения защиты данных и защиты информационных систем ООО «Контур» от НСД.

10.13.2 Должны быть определены цели использования сети Интернет и

требования к процедуре использования ресурсов сети Интернет. Использование сети Интернет работников в личных целях должно быть строго запрещено.

10.13.3 Доступ к информационным сервисам сети Интернет предоставляется работникам ООО «Контур» только в случае производственной необходимости. Подключение к сети Интернет должно осуществляться только при организации защиты соединения путем установки МЭ и специальных программных средств защиты.

10.13.4 Разрешительные политики доступа в Интернет должны технически реализовываться специализированным программным обеспечением.

10.13.5 Контроль использования работниками ресурсов сети Интернет должен осуществляться уполномоченными работниками на постоянной основе.

10.14 Использование корпоративной электронной почты

10.14.1 Система корпоративной электронной почты должна использоваться в ООО «Контур» с целью организации обмена электронными сообщениями между работниками, а также между работниками ООО «Контур» и внешними абонентами.

10.14.2 В ООО «Контур» должны быть четко определены требования к использованию системы корпоративной электронной почты.

10.14.3 Предоставление и прекращение доступа к ресурсам корпоративной электронной почты должно осуществляться только на основе оформленной заявки.

10.14.4 В ООО «Контур» должно быть установлено специальное программное обеспечение, осуществляющее контроль всех входящих сообщений на наличие вредоносного программного обеспечения.

10.14.5 В ООО «Контур» должны быть предусмотрены механизмы архивирования и резервного копирования корпоративной электронной почты в автоматическом режиме.

10.15 Резервное копирование и восстановление данных

10.15.1 Осуществление резервного копирования для:

- файловых серверов и серверов приложений, критичных для деятельности ООО «Контур»;
- операционных систем файловых серверов и прикладных программ;
- приложений, критичных для деятельности ООО «Контур»;
- рабочих данных.

10.15.2 Частота и режим резервного копирования устанавливаются таким образом, чтобы обеспечить минимальную потерю данных и допустимое время восстановления.

10.15.3 Резервное копирование и восстановление ресурсов информационных систем ООО «Контур» должны проводить уполномоченные работники ООО «Контур».

10.15.4 Резервное копирование должно осуществляться в автоматическом режиме с применением специализированного программно-аппаратного комплекса.

11 Основные требования к процессам управления информационной безопасностью

11.1 Управление рисками

11.1.1 Выбор требований по информационной безопасности и защитных механизмов, применяемых в системе информационной безопасности, должен основываться на проведении анализа рисков нарушения основных свойств безопасности для наиболее критичных информационных ресурсов ООО «Контур».

11.1.2 Основой оценки рисков должна быть оценка условий и факторов, которые могут стать причиной нарушения свойств целостности, конфиденциальности и доступности для ресурсов информационной системы ООО «Контур».

11.1.3 Результатом проведения анализа рисков должен быть комплекс мер, направленных на снижение возможного негативного влияния на основную деятельность ООО «Контур» при реализации той или иной угрозы и обеспечивающих достаточный

уровень защищенности информационных систем ООО «Контур».

11.2 Управление инцидентами информационной безопасности

11.2.1 Для обеспечения эффективного разрешения инцидентов информационной безопасности в ООО «Контур», минимизации потерь и уменьшения риска возникновения повторных инцидентов должно осуществляться эффективное управление инцидентами информационной безопасности. Для управления инцидентами информационной безопасности должна быть создана система учета произошедших инцидентов, которая представляет собой комплекс средств и мероприятий для сбора и консолидации информации об инцидентах.

11.2.2 В отношении каждого произошедшего инцидента должен выполняться его анализ и разработка эффективных мер реагирования на данный инцидент.

11.3 Мониторинг текущего уровня информационной безопасности

11.3.1 Для обеспечения высокого уровня контроля в отношении системы обеспечения информационной безопасности в ООО «Контур» на постоянной основе должен проводиться комплексный анализ существующих защитных механизмов и возникающих инцидентов информационной безопасности, а также периодический аудит всей системы обеспечения информационной безопасности.

11.3.2 Процесс мониторинга системы обеспечения информационной безопасности должен включать в себя контроль организационных и технических защитных мер, анализ параметров конфигурации и настройки защитных механизмов.

11.3.3 При проведении контрольных мероприятий, связанных с оценкой функционирования защитных мер в ООО «Контур», уполномоченные работники должны придерживаться следующих принципов:

- не нарушать функционирование текущей деятельности ООО «Контур»;
- действовать в соответствии с внутренними документами ООО «Контур» по информационной безопасности;
- не скрывать факты выявленных инцидентов и нарушений требований информационной безопасности;
- оформлять отчеты, подтверждающие выполнение мероприятий по обеспечению информационной безопасности.

11.3.4 Информация, полученная в ходе проведения контролирующих мероприятий о действиях, событиях и параметрах, имеющих отношение к функционированию защитных мер, должна консолидироваться и храниться в местах, исключающих получение к ней несанкционированного доступа.

11.3.5 Мониторинг данных о зарегистрированных событиях информационной безопасности должен проводиться, по возможности, с использованием встроенных механизмов настройки и аудита событий в программных и программно-технических средствах, используемых в информационных системах ООО «Контур».

11.4 Аудит системы обеспечения информационной безопасности

11.4.1 В целях оценки текущего уровня информационной безопасности уполномоченные работники ООО «Контур» на регулярной основе должны проводить аудит информационной безопасности.

11.4.2 Внутренние аудиты или самооценки должны выполняться, по возможности, работниками ООО «Контур».

11.4.3 Результатом выполнения аудитов по информационной безопасности должны стать отчеты о выполненном аудите информационной безопасности, которые разрабатываются специалистами ООО «Контур».

11.4.4 По результатам аудита уполномоченные работники и ответственные подразделения ООО «Контур» должны определить действия, необходимые для устранения обнаруженных несоответствий в процессе аудита и вызвавших их причин.

11.5 Управление персоналом

11.5.1 Организация такого процесса управления персоналом, который обеспечит доверительное отношение к работникам, а также организует комплексное противодействие угрозам информационной безопасности, исходящим от персонала ООО «Контур».

11.5.2 Выполнение обязательных проверок при приеме новых работников на работу с точки зрения достоверности сообщаемых ими данных и с позиции оценки их профессиональных навыков.

11.5.3 Организация работы в направлении повышения осведомленности и обучения в области информационной безопасности.

11.5.4 Повышение осведомленности работников ООО «Контур»:

– по существующим в ООО «Контур» политикам информационной безопасности;

– по применяемым в ООО «Контур» защитным мерам;

– по правильному использованию защитных мер в соответствии с внутренними документами ООО «Контур».

12 Заключение

12.1 Настоящая Политика является внутренним документом администрации, общедоступной и подлежит размещению на официальном сайте администрации.

12.2 Настоящая Политика подлежит изменению, дополнению в случае появления новых законодательных актов и специальных нормативных документов по обработке и защите персональных данных, но не реже одного раза в три года. При внесении изменений в актуальной редакции указывается дата последнего обновления. Новая редакция Политики вступает в силу с момента ее размещения, если иное не предусмотрено новой редакцией Политики. Действующая редакция всегда находится на странице по адресу: https://kontur61.com/wp-content/uploads/2024/05/politika_informacionnoj_bezopasnosti.pdf

12.3 Контроль исполнения требований настоящей Политики осуществляется ответственным лицом за обеспечение безопасности персональных данных администрации.

12.4 Ответственность должностных лиц администрации, имеющих доступ к конфиденциальной информации, за невыполнение требований норм, регулирующих обработку и защиту информации, определяется в соответствии с законодательством Российской Федерации и внутренними документами администрации.