Утверждаю:

Генеральный директор

ООО «Клиника Доктор КИТ»

_____ В.Ш. Пашаян

Положение об организации и обеспечении безопасности персональных данных

ООО «Клиника Доктор КИТ»

Ставрополь

2021

СОДЕРЖАНИЕ

СОКРАЩЕНИЯ И УСЛОВНЫЕ ОБОЗНАЧЕНИЯ

АРМ Автоматизированное рабочее место

ИСПДн Информационная система персональных данных

ПДн Персональные данные

СЗПДн Система защиты персональных данных

ФСБ России Федеральная служба безопасности России

ФСТЭК России Федеральная служба по техническому и экспортному контролю России

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Администратор информационной системы персональных данных (Администратор ИСПДн) – пользователь, уполномоченный выполнять некоторые действия (имеющий полномочия) по администрированию (управлению) информационной системой персональных данных в соответствии с установленной ролью.

Администратор системы защиты персональных данных (Администратор СЗПДн) – пользователь, уполномоченный выполнять некоторые действия (имеющий полномочия) по администрированию (управлению) системы защиты персональных данных в соответствии с установленной ролью.

Анализ уязвимостей – мероприятия по выявлению, идентификации и оценке уязвимостей ИСПДн в интересах определения возможности реализации угроз безопасности информации и способов предотвращения ущерба. Аутентификационная информация [информация аутентификации] – информация, используемая для установления подлинности (верификации) субъекта доступа в информационной системе персональных данных.

Аутентификация – проверка принадлежности субъекту доступа предъявленного им идентификатора (подтверждение подлинности субъекта доступа в информационной системе персональных данных).

Виртуализация – технология преобразование формата или параметров программных или сетевых запросов к компьютерным ресурсам с целью обеспечения независимости процессов обработки информации от программной или аппаратной платформы информационной системы персональных данных. Виртуальная машина – вычислительная система, эмулируемая с помощью технологии виртуализации, в которой установлена гостевая операционная система и обеспечивается выполнение прикладного программного обеспечения. Внешняя информационная система – информационная система, взаимодействующая с информационной системой персональных данных оператора из-за пределов границ информационной системы персональных данных оператора. Внешняя информационно-телекоммуникационная сеть – информационно-телекоммуникационная сеть, взаимодействующая с информационной системой персональных данных оператора из-за пределов границ информационной системы персональных данных оператора. Гипервизор – программа (программное обеспечение), создающая среду функционирования других программ (в том числе других гипервизоров) за счёт имитации аппаратных средств вычислительной техники, управления данными средствами и гостевыми операционными системами, функционирующими в данной среде.

Гостевая операционная система – операционная система, установленная на виртуальной машине. Доверенная загрузка – загрузка операционной системы средства вычислительной техники с заранее определенных постоянных машинных носителей при обязательном успешном прохождении процедур проверки целостности программной и аппаратной среды и идентификации и аутентификации. Доступность информации – свойство безопасности информации, при котором субъекты доступа, имеющие права доступа, могут беспрепятственно их реализовать. Защищенные линии связи – линии (каналы) связи, при передаче информации по которым обеспечивается требуемый уровень ее защищенности (конфиденциальность, целостность и (или) доступность информации). Идентификатор – представление (строка символов), однозначно идентифицирующее субъект и (или) объект доступа в информационной системе персональных данных. Идентификация – присвоение субъектам доступа, объектам доступа идентификаторов (уникальных имен) и (или) сравнение предъявленного идентификатора с перечнем присвоенных идентификаторов. Информационная система персональных данных (ИСПДн) – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств. Компонент программного обеспечения – составная часть (программный модуль) программного обеспечения, выполняющая определенную функцию .Компонент информационной системы персональных данных – часть информационной системы персональных данных, включающая некоторую совокупность информации и обеспечивающих ее обработку отдельных информационных технологий и технических средств. Компьютерный инцидент – непредвиденное или нежелательное событие (группа событий) безопасности, которое привело (могут привести) к нарушению функционирования информационной системы персональных данных или возникновению угроз безопасности информации (нарушению конфиденциальности, целостности, доступности). Контролируемая зона – пространство (территория, здание, часть здания), в котором исключено неконтролируемое пребывание лиц, а также транспортных, технических или иных средств. Конфиденциальность информации – свойство безопасности информации, при котором доступ к ней осуществляют только субъекты доступа, имеющие на него право. Лица, допущенные к обработке персональных данных – работники структурных подразделений и иные лица, допущенные к обработке персональных данных, в соответствии с приказом руководителя организации. Локальный доступ – доступ субъектов доступа к объектам доступа, осуществляемый непосредственно через подключение (доступ) к компоненту

информационной системы персональных данных или через локальную вычислительную сеть (без использования информационно-телекоммуникационной сети).Объект доступа – единица информационного ресурса информационной системы персональных данных (файл, техническое средство, узел сети, линия (канал) связи, мобильное устройство, программа, том, каталог, запись, поле записей и иные объекты), доступ к которой регламентируется правилами разграничения доступа и по отношению к которой субъекты доступа выполняют операции. Оператор персональных данных (оператор) – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции),совершаемые с персональными данными. Под оператором персональных данных в настоящем Положении понимается Общество с ограниченной ответственностью «Клиника Доктор КИТ», (далее – ООО «Клиника Доктор КИТ» Периметр информационной системы персональных данных – физическая и (или) логическая граница информационной системы персональных данных (сегмента информационной системы персональных данных), в пределах которой оператором обеспечивается защита информации в соответствии с едиными правилами и процедурами, а также контроль за реализованными мерами защиты информации. Персональные данные (ПДн) – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных). Пользователь – лицо, которому разрешено выполнять некоторые действия (операции) по обработке информации в информационной системе персональных данных или использующее результаты ее функционирования. Привилегированная учетная запись – учетная запись администратора информационной системы персональных данных. Программная среда – совокупность программного обеспечения, используемого в информационной системе персональных данных для решения одной или нескольких задач. Роль – предопределенная совокупность правил, устанавливающих допустимое взаимодействие между пользователем и информационной системой персональных данных. Сегмент информационной системы персональных данных – совокупность нескольких компонентов информационной системы персональных данных, использующих общую (в том числе разделяемую) среду передачи и объединенных для единства решения функциональных задач. Система защиты персональных данных (СЗПДн) – комплекс организационных и (или) технических мер, определенных с учетом актуальных угроз безопасности персональных данных и информационных технологий, используемых в информационных системах персональных данных.

Событие безопасности (информационной) – идентифицированное возникновение состояния информационной системы персональных данных (сегмента, компонента информационной системы персональных данных), сервиса или сети, указывающее на возможное нарушение безопасности информации, или сбой средств защиты информации, или ранее неизвестную ситуацию, которая может быть значимой для безопасности информации. Субъект доступа – пользователь, процесс, выполняющие операции (действия) над объектами доступа и действия которых регламентируются правилами разграничения доступа. Техническое средство – аппаратное или программно-аппаратное устройство, осуществляющее формирование, обработку, передачу или прием информации в информационной системе персональных данных.

Удаленный доступ – процесс получения доступа (через внешнюю сеть) к объектам доступа информационной системы персональных данных из другой информационной системы (сети) или со

средства вычислительной техники, не являющегося постоянно (непосредственно) соединенным физически или логически с информационной системой, к которой он получает доступ.

Управление доступом – ограничение и контроль доступа субъектов доступа к объектам доступа в информационной системе персональных данных в соответствии с установленными правилами разграничения доступа. Устройство – конструктивно законченный технический элемент, имеющий определенное функциональное назначение в информационной системе персональных данных. Уязвимость информационной системы персональных данных – недостаток (слабость) информационной системы персональных данных, который (которая) создает потенциальные или реально существующие условия для реализации или проявления угроз безопасности информации.

Целостность информации – свойство безопасности информации, при котором отсутствует любое ее изменение либо изменение субъектами доступа, имеющими на него право.

1 ОБЩИЕ ПОЛОЖЕНИЯ

1.1 Назначение

Настоящий документ «ООО Клиника Доктор КИТ» Положение об организации и обеспечении безопасности персональных данных» (далее – Положение) устанавливает состав и содержание организационных мер по обеспечению безопасности ПДн при их обработке в ИСПДн, разработанных и внедренных в рамках созданной СЗПДн в соответствии с требованиями Приказа ФСТЭК России от 18.02.2013 No 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

1.2 Область действия

Действие настоящего Положения распространяется на все структурные подразделения ООО «Клиника Доктор КИТ» г. Ставрополя, осуществляющие обработку ПДн в ИСПДн, а также лиц, обеспечивающих функционирование (сопровождение, обслуживание, ремонт), управление (администрирование) ИСПДн и СЗПДн ООО «Клиника Доктор КИТ» Ознакомление работников ООО «Клиника Доктор КИТ» г. Ставрополя с настоящим Положением, а также контроль исполнения настоящего Положения осуществляет лицо, ответственное за организацию обработки ПДн в соответствии с документом ООО «Клиника Доктор КИТ»

Инструкция лица, ответственного за организацию обработки персональных данных».

1.3 Нормативно-правовая основа Настоящее Положение разработано на основании и с учетом следующих нормативных правовых актов:

− Федеральный закон РФ от 27.07.2006 No 152-ФЗ «О персональных данных»; − Постановление Правительства РФ от 01.11.2012 No 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

− Постановление Правительства РФ от 15.09.2008 No 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

− Приказ ФСТЭК России от 18.02.2013 No 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

− Приказ ФСБ России от 10.07.2014 No 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».

2 ОРГАНИЗАЦИОННАЯ СТРУКТУРА ОБЕСПЕЧЕНИЯ

БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Безопасность ПДн при их обработке в ИСПДн обеспечивает оператор или лицо, осуществляющее обработку ПДн по поручению оператора, в соответствии с законодательством Российской Федерации. В ООО «Клиника Доктор КИТ» г. Ставрополя для обеспечения безопасности ПДн определены следующие лица:

− лицо, ответственное за организацию обработки ПДн (далее – Ответственный за организацию обработки ПДн);

- лицо, ответственное за обеспечение безопасности ПДн (далее –Ответственный за обеспечение безопасности ПДн);

− лицо (лица), обеспечивающее функционирование (сопровождение,

обслуживание, ремонт) СЗПДн (далее – Администратор СЗПДн);

− лицо (лица), обеспечивающее управление (администрирование) ИСПДн

(далее – Администратор ИСПДн);

− лица, допущенные к обработке ПДн в ИСПДн (далее – Пользователи ИСПДн). Для выполнения работ по обеспечению безопасности ПДн при их обработке оператор может привлекать на договорной основе организации имеющие лицензию на деятельность по технической защите конфиденциальной информации.

2.1 Ответственный за организацию обработки персональных данных

Ответственный за организацию обработки ПДн осуществляет следующие функции в части обеспечения безопасности ПДн:

− совместно с Ответственным за обеспечение безопасности ПДн и другими должностными лицами ООО «Клиника Доктор КИТ» принимает участие в определении уровня защищенности ПДн в ИСПДн;

− совместно с Ответственным за обеспечение безопасности ПДн и другими должностными лицами ООО «Клиника Доктор КИТ» принимает участие в определении актуальных угроз безопасности ПДн при их обработке в ИСПДн;

− совместно с Ответственным за обеспечение безопасности ПДн и другими должностными лицами ООО «Клиника Доктор КИТ» принимает участие в формировании требований по обеспечению безопасности ПДн и формировании технических и организационных мер по обеспечению безопасности ПДн. При необходимости вносит предложения по корректировке набора организационных и технических мер по обеспечению безопасности ПДн;

− совместно с Ответственным за обеспечение безопасности ПДн, Администратором СЗПДн и другими должностными лицами ООО «Клиника Доктор КИТ» принимает участие в создании системы защиты персональных данных;

− осуществляет контроль соблюдения в ООО «Клиника Доктор КИТ» принципов обработки персональных данных;

− совместно с Ответственным за обеспечение безопасности ПДн, Администратором СЗПДн, Администратором ИСПДн участвует в проведении расследований случаев несанкционированного доступа к ПДн и других нарушений правил обработки ПДн;

− совместно с Ответственным за обеспечение безопасности ПДн и другими

должностными лицами ООО «Клиника Доктор КИТ» г. Ставрополя организует и

осуществляет процессы удаления и уничтожения ПДн;

− осуществляет иные процедуры, предусмотренные настоящим Положением.

Права, обязанности и функции Ответственного за организацию обработки ПДн определены в документе ООО «Клиника Доктор КИТ» Инструкция лица, ответственного за организацию обработки персональных данных».

2.2 Ответственный за обеспечение безопасности персональных данных

Ответственный за обеспечение безопасности ПДн осуществляет следующие

функции в части обеспечения безопасности ПДн:

− совместно с Ответственным за организацию обработки ПДн и другими

должностными лицами ООО «Клиника Доктор КИТ» г. Ставрополя принимает участие в

определении уровня защищенности ПДн в ИСПДн;

− совместно с Ответственным за организацию обработки ПДн и другими должностными лицами ООО «Клиника Доктор КИТ» принимает участие в определении актуальных угроз безопасности ПДн при их обработке в ИСПДн;

− совместно с Ответственным за организацию обработки ПДн и другими должностными лицами ООО «Клиника Доктор КИТ» принимает участие в формировании требований по обеспечению безопасности ПДн и

формировании технических и организационных мер по обеспечению безопасности ПДн. При необходимости вносит предложения по корректировке набора организационных и технических мер по обеспечению безопасности ПДн;

− совместно с Ответственным за организацию обработки ПДн, Администратором СЗПДн и другими должностными лицами ООО «Клиника Доктор КИТ» принимает участие в создании системы защиты ПДн;

− совместно с Ответственным за организацию обработки ПДн, Администратором СЗПДн, Администратором ИСПДн участвует в проведении расследований случаев несанкционированного доступа к ПДн и других нарушений правил обработки ПДн;

− совместно с Ответственным за организацию обработки ПДн и другими должностными лицами ООО «Клиника Доктор КИТ» организует и осуществляет процессы удаления и уничтожения ПДн;

− осуществляет иные процедуры, предусмотренные настоящим Положением. Права, обязанности и функции Ответственного за обеспечение безопасности ПДн определены в документе ООО «Клиника Доктор КИТ» Инструкция лица, ответственного за обеспечение безопасности персональных данных».

2.3 Администратор системы защиты персональных данных Администратор СЗПДн осуществляет следующие функции в части обеспечения безопасности ПДн:

− совместно с Ответственным за организацию обработки ПДн, Ответственным за обеспечение безопасности ПДн и другими должностными лицами ООО «Клиника Доктор КИТ» принимает участие в создании системы защиты персональных данных;

− совместно с Ответственным за организацию обработки ПДн, Ответственным за обеспечение безопасности ПДн, Администратором ИСПДн участвует в проведении расследований случаев несанкционированного доступа к ПДн и других нарушений правил обработки ПДн;

− обеспечивает функционирование (сопровождение, обслуживание, ремонт) и

управление (администрирование) СЗПДн ООО «Клиника Доктор КИТ»

(средств защиты информации, входящих в состав СЗПДн, компонентов

ИСПДн, реализующих функции по обеспечению безопасности ПДн);

− осуществляет иные процедуры, предусмотренные настоящим Положением.

Права, обязанности и функции Администратора СЗПДн определены в документе ООО «Клиника Доктор КИТ». Руководство администратора системы защиты персональных данных».

2.4 Администратор информационной системы персональных данных Администратор ИСПДн осуществляет следующие функции в части обеспечения безопасности ПДн:

− совместно с Ответственным за организацию обработки ПДн, Ответственным

за обеспечение безопасности ПДн, Администратором СЗПДн участвует в

проведении расследований случаев несанкционированного доступа к ПДн и

других нарушений правил обработки ПДн;

− обеспечивает функционирование (сопровождение, обслуживание, ремонт) и управление (администрирование) ИСПДн ООО «Клиника Доктор КИТ»;

− осуществляет иные процедуры, предусмотренные настоящим Положением.

Права, обязанности и функции Администратора ИСПДн определены в документе ООО «Клиника Доктор КИТ» Инструкция администратора информационной системы персональных данных».

2.5 Пользователь информационной системы персональных данных

Пользователь ИСПДн осуществляет следующие функции в части обеспечения безопасности ПДн:

− эксплуатирует ИСПДн и СЗПДн (средства защиты информации, входящие в состав СЗПДн) в зоне своей ответственности;

− осуществляет иные процедуры, предусмотренные настоящим Положением.

Права, обязанности и функции Пользователя ИСПДн определены в документе ООО «Клиника Доктор КИТ» Инструкция пользователя информационной системы персональных данных».

3 ОРГАНИЗАЦИОННЫЕ МЕРЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

В ООО «Клиника Доктор КИТ» г. Ставрополя реализован комплекс технических и организационных мер защиты информации, включающий в том числе следующие организационные меры обеспечения безопасности ПДн:

− 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, на которых хранятся и (или)

обрабатываются ПДн (далее - машинные носители ПДн) (ЗНИ);

− регистрация событий безопасности (РСБ);

− антивирусная защита (АВЗ);

− обнаружение вторжений (СОВ);

− контроль (анализ) защищенности ПДн (АНЗ);

− обеспечение целостности ИСПДн и ПДн (ОЦЛ);

− обеспечение доступности ПДн (ОДТ);

− защита среды виртуализации (ЗСВ);

− защита технических средств (ЗТС);

− защита ИСПДн, ее средств, систем связи и передачи данных (ЗИС);

− выявление инцидентов (одного события или группы событий), которые могут

привести к сбоям или нарушению функционирования ИСПДн и (или) к возникновению угроз безопасности ПДн (далее – компьютерные инциденты), и реагирование на них (ИНЦ);

− управление конфигурацией ИСПДн и СЗПДн (УКФ).

Указанные выше организационные меры реализованы в комплексе с техническими мерами обеспечения безопасности ПДн при их обработке в ИСПДн виде соответствующих подсистем СЗПДн.

3.1 Подсистема идентификации и аутентификации субъектов

доступа и объектов доступа (ИАФ)

Подсистема идентификации и аутентификации субъектов доступа и объектов доступа обеспечивает 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).

3.1.1 Идентификация и аутентификация пользователей, являющихся

работниками оператора (внутренних пользователей) (ИАФ.1)

При доступе в ИСПДн осуществляется идентификация и аутентификация пользователей, являющихся работниками ООО «Клиника Доктор КИТ», (внутренних пользователей) с использованием учетных данных (логин и пароль) и процессов, запускаемых от имени этих пользователей, а также процессов, запускаемых от имени системных учетных записей.

К внутренним пользователям ИСПДн относятся должностные лица ООО «Клиника Доктор КИТ»,

выполняющие свои должностные обязанности (функции) с использованием информации (включая ПДн), информационных технологий и технических средств ИСПДн в соответствии с должностными регламентами (инструкциями), утвержденными ООО «Клиника Доктор КИТ» г. Ставрополя, и которым в ИСПДн могут быть присвоены следующие учетные записи в зависимости от их полномочий:

− Ответственный за организацию обработки ПДн;

− Ответственный за обеспечение безопасности ПДн;

− Администратор СЗПДн;

− Администратор ИСПДн;

− Пользователь ИСПДн.

Однозначное сопоставление идентификатора пользователя с запускаемыми от его имени процессами осуществляется средствами защиты информации. Однозначная идентификация и аутентификация обеспечивается для всех видов доступа, кроме тех видов доступа, которые определяются как действия, разрешенные до идентификации и аутентификации в соответствии с пунктом 3.2.8 настоящего Положения (УПД.11).

3.1.2 Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных (ИАФ.2)

В ИСПДн до начала информационного взаимодействия (передачи защищаемой информации от устройства к устройству) осуществляется идентификация и аутентификация устройств (технических средств) с использованием соответствующих протоколов аутентификации или с применением криптографических методов защиты информации.

Перечень типов устройств, используемых в ИСПДн и подлежащих идентификации и аутентификации до начала информационного взаимодействия, определяется совместно Ответственным за обеспечение безопасности ПДн, Администратором СЗПДн, Администратором ИСПДн и включает:

− коммуникационное оборудование;

− серверное оборудование;

− автоматизированные рабочие места (стационарный компьютер, ноутбук и

т.д.);

− мобильные устройства.

Идентификация устройств в ИСПДн обеспечивается по логическим именам (имя устройства и (или) ID), логическим адресам (например, IP-адресам) и (или) по физическим адресам (например, MAC-адресам) устройства или по комбинации имени, логического и (или) физического адресов устройства.

3.1.3 Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов (ИАФ.3)

Создание, присвоение и уничтожение идентификаторов пользователей и

устройств осуществляется:

− Администратором СЗПДн с использованием средств защиты информации

соответствии с документом ООО «Клиника Доктор КИТ».Руководство администратора системы защиты персональных данных»;

− Администратором ИСПДн с использованием встроенных средств общесистемного или прикладного программного обеспечения в соответствии с документом ООО «Клиника Доктор КИТ» Инструкция администратора информационной системы персональных данных.

Присвоение идентификаторов пользователей осуществляется в соответствии с порядком, указанном в пунктах 3.2.1.2 и 3.2.1.3 настоящего Положения (УПД.1).

При создании, присвоении и уничтожении идентификаторов пользователей и устройств Администратором СЗПДн и Администратором ИСПДн учитываются следующие ограничения использования:

− идентификатор должен однозначно идентифицировать пользователя и (или) устройство;

− повторное использование идентификатора пользователя и (или) устройства

исключается (в течение не менее одного года);

− блокирование идентификатора пользователя осуществляется через

установленный период неиспользования (не более 90 дней);

− при создании учетной записи пользователя ИСПДн исключено использование идентификатора пользователя, используемого в публичной электронной почте или иных публичных сервисах.

3.1.4 Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации (ИАФ.4)

Хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации осуществляется:

− Администратором СЗПДн с использованием средств защиты информации в соответствии с документом ООО «Клиника Доктор КИТ» Руководство администратора системы защиты персональных данных»;

− Администратором ИСПДн с использованием встроенных средств общесистемного или прикладного программного обеспечения в соответствии с документом ООО «Клиника Доктор КИТ» Инструкция администратора информационной системы персональных данных.

Выдача средств аутентификации пользователям осуществляется в соответствии

с порядком, указанном в пунктах 3.2.1.2 и 3.2.1.3 настоящего Положения (УПД.1).

Администратором СЗПДн и Администратором ИСПДн осуществляется:

− изменение аутентификационной информации (средств аутентификации),

заданных их производителями и (или) используемых при внедрении СЗПДн;

− генерация и выдача начальной аутентификационной информации (начальных

значений средств аутентификации);

− назначение необходимых характеристик средств аутентификации (в том числе механизма пароля) в зависимости от особенностей функционирования ИСПДн:

о длина и алфавит пароля (длина не менее 6 символов, алфавит не менее 70 символов);

о минимальное количество измененных символов при создании новых паролей (не менее одного символа);

о максимальное количество неуспешных попыток аутентификации (ввода неправильного пароля) до блокировки входа в ИСПДн (доступа к ИСПДн) за установленный период времени (3 попытки, блокировка при достижении установленного максимального количества неуспешных попыток аутентификации − 10 минут);

о максимальное время действия пароля (90 дней);

о запрет на использование пользователями ИСПДн последних использованных паролей при создании новых паролей.

− блокирование (прекращение действия) и замена утерянных,

скомпрометированных или поврежденных средств аутентификации.

Пользователями ИСПДн осуществляется:

− смена начального аутентификатора (пароля) на новый после первого подключения к ИСПДн;

− обновление аутентификатора (пароля) с установленной периодичностью;

− защита аутентификационной информации от неправомерного доступа к ней и модифицирования.

3.1.5 Защита обратной связи при вводе аутентификационной информации (ИАФ.5)

В ИСПДн ООО «Клиника Доктор КИТ» в процессе аутентификации обеспечивается исключением в средствах защиты информации, в прикладном и общесистемном программном обеспечении отображения для пользователя действительного значения аутентификационной информации. Вводимые символы пароля отображаются условными знаками.

3.1.6 Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей) (ИАФ.6)

При доступе в ИСПДн осуществляется однозначная идентификация и аутентификация пользователей, не являющихся работниками ООО «Клиника Доктор КИТ» (внешних пользователей), или процессов, запускаемых от имени этих пользователей.

К пользователям, не являющимся работниками ООО «Клиника Доктор КИТ» (внешним пользователям), относятся все пользователи ИСПДн, не указанные в качестве внутренних пользователей в пункте 3.1.1 настоящего Положения (ИАФ.1). Внешние пользователи ИСПДн однозначно идентифицируются и аутентифицируются для всех видов доступа, кроме тех видов доступа, которые определяются как действия, разрешенные до идентификации и аутентификации в соответствии с пунктом 3.2.8 настоящего Положения (УПД.11).

3.2 Подсистема управления доступом субъектов доступа к объектам доступа (УПД) Подсистема управления доступом субъектов доступа к объектам доступа обеспечивает управление правами и привилегиями субъектов доступа, разграничение доступа субъектов доступа к объектам доступа на основе совокупности установленных в ИСПДн правил разграничения доступа, а также обеспечивает контроль за соблюдением этих правил.

3.2.1 Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей (УПД.1)

3.2.1.1 Общие правила и процедуры управления учетными записями пользователей Верификация пользователя (проверка личности пользователя, его должностных (функциональных) обязанностей) для заведения учетной записи пользователя и определение типа учетной записи (внутреннего пользователя, внешнего пользователя; системная, приложения; гостевая (анонимная), временная и (или) иные типы записей) осуществляется Ответственным за обеспечение безопасности ПДн при

получении Заявки на предоставление/изменение прав доступа (далее – Заявки),

форма которой приведена в приложении к настоящему Положению Администратором СЗПДн и (или) Администратором ИСПДн осуществляется предоставление пользователям прав доступа к объектам доступа ИСПДн,основываясь на задачах, решаемых пользователями в ИСПДн на основании Заявки,согласованной Ответственным за обеспечение безопасности ПДн.

Пользователям ИСПДн должны предоставляться минимально необходимые для выполнения должностных (функциональных) обязанностей права доступа в ИСПДн.

Ответственность за минимальную достаточность прав доступа и за соответствие уровня допуска задачам, решаемым внутренним или внешним пользователем, несут работники, являющиеся инициаторами создания Заявок.

Контроль, пересмотр и изменение (корректировка) прав доступа пользователей осуществляется Ответственным за обеспечение безопасности ПДн в рамках проводимых регулярных мероприятий по мониторингу и контролю обработки ПДн в соответствии с документом ООО «Клиника Доктор КИТ» Инструкция лица, ответственного за обеспечение безопасности персональных данных».

Администратором СЗПДн совместно с Администратором ИСПДн реализуются следующие функции управления учетными записями пользователей, в том числе внешних пользователей:

− объединение учетных записей в группы (при необходимости);

− заведение, активация, блокирование и уничтожение учетных записей пользователей;

− пересмотр и, при необходимости, корректировка учетных записей пользователей с установленной периодичностью;

− заведение и контроль использования гостевых (анонимных) и временных учетных записей пользователей, а также привилегированных учетных записей администраторов;

− контроль за изменениями сведений о пользователях, их ролях, обязанностях, полномочиях, ограничениях;

− уничтожение временных учетных записей пользователей, предоставленных для однократного (ограниченного по времени) выполнения задач в ИСПДн.

3.2.1.2 Управление учетными записями внутренних пользователей. Руководитель структурного подразделения работника ООО «Клиника Доктор КИТ», доступ которому в ИСПДн необходим для выполнения должностных (функциональных) обязанностей, направляет Ответственному за обеспечение безопасности ПДн Заявку, содержащую следующую информацию:

− фамилия, имя, отчество работника;

− должность работника;

− контактная информация;

− обоснование служебной необходимости предоставления прав доступа (полномочий) в ИСПДн;

− сведения о необходимых правах доступа (полномочиях) в ИСПДн;

− иная дополнительная информация (необходимость предоставления

удаленного доступа или использования съемных машинных носителей информации).

После согласования Ответственным за обеспечение безопасности ПДн, предоставляемых прав доступа и полномочий Администратором СЗПДн и (или) Администратором ИСПДн осуществляется заведение работнику учетной записи пользователя не позднее 2 (двух) рабочих дней со дня получения Заявки.

В случае необходимости изменения (корректировки) прав доступа внутренним пользователям, обладающим учетными записями в ИСПДн, руководитель структурного подразделения работника, которому требуется изменение прав доступа, направляет Ответственному за обеспечение безопасности ПДн Заявку, содержащую следующую информацию:

− фамилия, имя, отчество работника;

− должность работника;

− контактная информация;

− обоснование служебной необходимости изменения прав доступа (полномочий) в ИСПДн;

− необходимые права доступа (полномочия) в ИСПДн;

− иная дополнительная информация (необходимость предоставления удаленного доступа или использования съемных машинных носителей информации).

После согласования Ответственным за обеспечение безопасности ПДн изменения прав доступа и полномочий Администратором СЗПДн и (или) Администратором ИСПДн осуществляется изменение прав доступа учетной записи пользователя не позднее 2 (двух) рабочих дней со дня получения Заявки.

3.2.1.3 Управление учетными записями внешних пользователей Временная учетная запись может быть заведена для лица, не являющегося работником ООО «Клиника Доктор КИТ», на

ограниченный срок для выполнения задач, требующих расширенных полномочий, или для проведения настройки, тестирования ИСПДн, для организации гостевого доступа (посетителям, работникам сторонних организаций, стажерам и иным пользователям с временным доступом к ИСПДн).

В случае необходимости создания (изменения) учетной записи в ИСПДн для лица, не являющегося работником ООО «Клиника Доктор КИТ», работник ООО «Клиника Доктор КИТ» взаимодействующий с лицом, не являющимся работником ООО «Клиника Доктор КИТ» обязан направить Ответственному за обеспечение безопасности ПДн Заявку, содержащую следующую информацию:

− фамилия, имя, отчество лица, не являющегося работником ООО «Клиника Доктор КИТ»;

− наименование организации (при наличии);

− контактная информация лица, не являющегося работником ООО «Клиника Доктор КИТ»

− обоснование необходимости предоставления (изменения) прав доступа в ИСПДн;

− сведения о необходимых правах доступа (полномочиях) в ИСПДн;

− иная дополнительная информация (необходимость предоставления удаленного доступа или использования съемных машинных носителей информации);

− срок действия учетной записи внешнего пользователя.

После согласования Ответственным за обеспечение безопасности ПДн предоставляемых прав (изменений прав) доступа и полномочий Администратором СЗПДн и (или) Администратором ИСПДн осуществляется создание учетной записи (изменение прав доступа) пользователя не позднее 2 (двух) рабочих дней со дня получения Заявки.

3.2.1.4 Порядок прекращения доступа

Прекращение доступа внутреннего пользователя в ИСПДн осуществляется на основании Заявки Ответственному за обеспечение безопасности ПДн от работника или от руководителя структурного подразделения работника, аналогично порядку изменения прав доступа для внутренних пользователей.

Прекращение доступа внешнего пользователя в ИСПДн осуществляется на основании Заявки Ответственному за обеспечение безопасности ПДн от работника ООО «Клиника Доктор КИТ», взаимодействующего с лицом, не являющимся работником ООО «Клиника Доктор КИТ» Порядок прекращения прав доступа внешнего пользователя в ИСПДн аналогичен порядку прекращения доступа в ИСПДн для внутреннего пользователя.

Решение о прекращении доступа пользователя в ИСПДн может быть принято Ответственным за обеспечение безопасности ПДн или Ответственным за организацию обработки ПДн на основании локальных актов ООО «Клиника Доктор КИТ» а также на основании проводимых регулярных мероприятий по

мониторингу и контролю обработки ПДн в соответствии с документом ООО «Клиника Доктор КИТ».Инструкция лица, ответственного за обеспечение безопасности персональных данных».

Учетные записи пользователей с пометкой о готовности к удалению должны быть удалены Администратором ИСПДН или Администратором СЗПДн не ранее 6 (шести)месяцев со дня их отключения.

3.2.2 Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа (УПД.2)

В ИСПДн для управления доступом субъектов доступа к объектам доступа с учетом особенностей функционирования ИСПДн реализуется ролевой метод управления доступом, предусматривающий управление доступом субъектов доступа к объектам доступа на основе ролей субъектов доступа (совокупность действий и обязанностей, связанных с определенным видом деятельности).

Типы доступа включают операции по чтению, записи, удалению, выполнению и иные операции, разрешенные к выполнению пользователем (группе пользователей) или запускаемому от его имени процессу при доступе к объектам доступа.

Правила разграничения доступа к ИСПДн устанавливаются Администратором СЗПДн и (или) Администратором ИСПДн в зависимости от установленных должностных обязанностей пользователей и выполняемых ими задач и обеспечивают управление доступом пользователей (групп пользователей) и запускаемых от их имени процессов при входе в систему, доступе к техническим средствам, устройствам, объектам файловой системы, запускаемым и исполняемым модулям, объектам систем управления базами данных, объектам, создаваемым прикладным и специальным программным обеспечением, параметрам настройки средств защиты информации, информации о конфигурации СЗПДн и иной информации о функционировании СЗПДн, а также иным объектам доступа.

Доступ к указанной информации осуществляется в соответствии с пунктом 3.2.1

настоящего Положения (УПД.1) на основании разрешительной системы доступа,приведенной к настоящему Положению

3.2.3 Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами (УПД.3)

В ООО «Клиника Доктор КИТ» определены и зафиксированы в технических и эксплуатационных документах на СЗПДн способы и правила взаимодействия между сегментами сети, пользователями и устройствами в ИСПДн. Средствами СЗПДн осуществляется фильтрация информационных потоков в ИСПДн в соответствии с установленными правилами межсетевого экранирования. Осуществляется блокирование:

− передачи защищаемой информации через сеть Интернет по незащищенным линиям связи;

− сетевых запросов и трафика, несанкционированно исходящих из

информационной системы и (или) входящие в информационную систему.

В случае необходимости, создание (изменение) способов и правил взаимодействия, правил межсетевого экранирования осуществляется в соответствии с пунктом 3.15 настоящего Положения (УКФ).

3.2.4 Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы (УПД.4)

В ИСПДн обеспечивается разделение следующих полномочий (ролей):

− Администратор СЗПДн;

− Администратор ИСПДн;

− Пользователи ИСПДн.

Работники ООО «Клиника Доктор КИТ» Ставрополя назначаются на указанные роли

приказом руководителя ООО «Клиника Доктор КИТ» (или иного уполномоченного лица).

Права, обязанности и функции указанных лиц (ролей) определены в следующих документах:

− ООО «Клиника Доктор КИТ» Руководство администратора системы защиты персональных данных»;

− ООО «Клиника Доктор КИТ» Инструкция администратора информационной системы персональных данных»;

−ООО «Клиника Доктор КИТ» Инструкция пользователя информационной системы персональных данных».

Доступ к объектам доступа с учетом разделения полномочий (ролей)

обеспечивается в соответствии с пунктом 3.2.2 настоящего Положения (УПД.2).

3.2.5 Назначение минимально необходимых прав и привилегий

пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы (УПД.5)

При предоставлении прав доступа в ИСПДн, к техническим компонентам ИСПДн и к СЗПДн в ООО «Клиника Доктор КИТ» предоставляться минимально необходимые для выполнения должностных (функциональных) обязанностей права доступа.

Пользователям ИСПДн должны предоставляться минимально необходимые для выполнения должностных (функциональных) обязанностей права доступа в ИСПДн в соответствии с пунктом 3.2.1 настоящего Положения (УПД.1).

Права доступа администраторам и лицам, обеспечивающим функционирование ИСПДн и СЗПДн определяются при создании ИСПДн и СЗПДн.

В случае необходимости, изменение прав доступа пользователям, администраторам и лицам, обеспечивающим функционирование ИСПДн и СЗПДн

осуществляется в соответствии с пунктом 3.2.1 настоящего Положения (УПД.1).

3.2.6 Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе) (УПД.6)

В зависимости от особенностей функционирования ИСПДн Администратором СЗПДн и (или) Администратором ИСПДн устанавливается максимальное количество неуспешных попыток аутентификации (ввода неправильного пароля) до блокировки входа в ИСПДн (доступа к ИСПДн) за установленный период времени.

При превышении ограничения количества неуспешных попыток входа в ИСПДн (доступа к ИСПДн) средствами СЗПДн осуществляется блокирование устройства, с которого предпринимаются попытки доступа, и (или) учетной записи пользователя.

Ограничение количества неуспешных попыток входа в информационную систему

(доступа к ИСПДн) обеспечивается в соответствии с пунктом 3.1.4 настоящего Положения (ИАФ.4).

3.2.7 Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу (УПД.10)

В зависимости от особенностей функционирования ИСПДн Администратором СЗПДн и (или) Администратором ИСПДн устанавливается допустимый период бездействия (неактивности) пользователя, по истечении которого обеспечивается блокирование сеанса доступа пользователя в ИСПДн. Блокирование сеанса доступа пользователя в ИСПДн также осуществляется по запросу пользователя.

Блокирование сеанса доступа пользователя в ИСПДн обеспечивает временное приостановление работы пользователя со средством вычислительной техники, с которого осуществляется доступ к ИСПДн.

Для заблокированного сеанса должно осуществляться блокирование любых действий по доступу к информации и устройствам отображения, кроме необходимых для разблокирования сеанса.

Блокирование сеанса доступа пользователя в ИСПДн сохраняется до прохождения им повторной идентификации и аутентификации в соответствии с пунктом 3.1.1 настоящего Положения (ИАФ.1).

3.2.8 Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации (УПД.11)

Пользователям ИСПДн запрещаются любые действия в ИСПДн до прохождения процедуры идентификации и аутентификации.

Администратору СЗПДн, Администратору ИСПДн разрешаются действия в обход установленных процедур идентификации и аутентификации, необходимые только для восстановления функционирования ИСПДн в случае сбоев в работе или выходе из строя отдельных технических средств (устройств).

3.2.9 Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети (УПД.13)

Защита информации при доступе пользователей (процессов запускаемых от имени пользователей) и (или) иных субъектов доступа к объектам доступа ИСПДн через информационно-телекоммуникационные сети, в том числе сети связи общего пользования, реализуется с использованием средств СЗПДн в зависимости от особенностей функционирования ИСПДн.

Ответственным за обеспечение безопасности ПДн осуществляется установление (в том числе документальное) видов доступа, разрешенных для удаленного доступа к объектам доступа ИСПДн, и ограничение на использование удаленного доступа в соответствии с задачами (функциями) ИСПДн, для решения которых такой доступ необходим, и пунктом 3.2.2 настоящего Положения (УПД.2).

Защита удаленного доступа обеспечивается при всех видах доступа (беспроводной, проводной (коммутируемый), широкополосный и иные виды доступа). Администратором СЗПДн совместно с Администратором ИСПДн обеспечивается:

− предоставление удаленного доступа только тем пользователям, которым он необходим для выполнения установленных должностных обязанностей (функций) в соответствии с пунктом 3.2.1 настоящего Положения (УПД.1);

− мониторинг и контроль удаленного доступа на предмет выявления несанкционированного удаленного доступа к объектам доступа ИСПДн;

− контроль удаленного доступа пользователей (процессов запускаемых от имени пользователей) к объектам доступа ИСПДн до начала информационного взаимодействия с ИСПДн (передачи защищаемой информации).

Контроль и мониторинг использования удаленного доступа осуществляется Ответственным за обеспечение безопасности ПДн в рамках проводимых регулярных мероприятий по мониторингу и контролю обработки ПДн в соответствии с документом ООО «Клиника Доктор КИТ» Инструкция лица, ответственного за обеспечение безопасности персональных данных»

3.2.10 Регламентация и контроль использования в информационной системе технологий беспроводного доступа (УПД.14)

Регламентация и контроль использования технологий беспроводного доступа включает:

− ограничение на использование технологий беспроводного доступа (беспроводной передачи данных, беспроводного подключения оборудования к сети, беспроводного подключения устройств к средству вычислительной техники) в соответствии с задачами (функциями) ИСПДн, для решения

которых такой доступ необходим, и предоставление беспроводного доступа в соответствии с пунктом 3.2.2 настоящего Положения (УПД.2);

− предоставление технологий беспроводного доступа только тем пользователям, которым он необходим для выполнения установленных должностных обязанностей (функций) осуществляется в соответствии с пунктом 3.2.1 настоящего Положения (УПД.1);

− контроль беспроводного доступа пользователей (процессов запускаемых от имени пользователей) к объектам доступа ИСПДн до начала информационного взаимодействия с ИСПДн осуществляется в соответствии с пунктом 3.2.9 настоящего Положения (УПД.13).

Контроль и мониторинг использования технологий беспроводного доступа осуществляется Ответственным за обеспечение безопасности ПДн в рамках проводимых регулярных мероприятий по мониторингу и контролю обработки ПДн в соответствии с документом ООО «Клиника Доктор КИТ» Инструкция лица, ответственного за обеспечение безопасности персональных данных».

3.2.11 Регламентация и контроль использования в информационной системе мобильных технических средств (УПД.15)

В качестве мобильных технических средств рассматриваются съемные машинные носители информации (флэш-накопители, внешние накопители на жестких дисках и иные устройства), портативные вычислительные устройства и устройства связи с возможностью обработки информации (ноутбуки, нетбуки, планшеты, сотовые телефоны, цифровые камеры, звукозаписывающие устройства и иные устройства). Регламентация и контроль использования мобильных технических средств включают:

− установление (в том числе документальное) видов доступа (беспроводной, проводной (коммутируемый), широкополосный и иные виды доступа),разрешенных для доступа к объектам доступа ИСПДн с использованием мобильных технических средств, входящих в состав ИСПДн, в соответствии с пунктами 3.2.2, 3.2.10 настоящего Положения (УПД.2, УПД.14);

− ограничение на использование мобильных технических средств в соответствии с задачами (функциями) ИСПДн, для решения которых использование таких средств необходимо, и предоставление доступа с использованием мобильных технических средств в соответствии с пунктом 3.2.2 настоящего Положения (УПД.2);

− запрет возможности запуска без команды пользователя в ИСПДн программного обеспечения (программного кода), используемого для взаимодействия с мобильным техническим средством.

Контроль и мониторинг использования мобильных технических средств осуществляется Ответственным за обеспечение безопасности ПДн в рамках проводимых регулярных мероприятий по мониторингу и контролю обработки ПДн в соответствии с документом ООО «Клиника Доктор КИТ» Инструкция лица, ответственного за обеспечение безопасности персональных данных».

3.2.12 Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы) (УПД.16)

В ИСПДн осуществляется управление взаимодействием с информационными системами сторонних организаций (внешними информационными системами) и включает в себя:

− предоставление доступа к ИСПДн только авторизованным (уполномоченным) пользователям соответствии с пунктом 3.1.6 настоящего Положения (ИАФ.6);

− определение типов прикладного программного обеспечения ИСПДн, к которым разрешен доступ авторизованным (уполномоченным) пользователям из внешних информационных систем в соответствии с пунктом 3.2.2

настоящего Положения (УПД.2);

− определение системных учетных записей, используемых в рамках данного взаимодействия;

− определение порядка предоставления доступа к ИСПДн авторизованными (уполномоченным) пользователями из внешних информационных систем в соответствии с пунктом 3.2.1 настоящего Положения (УПД.1);

− определение порядка обработки, хранения и передачи информации с использованием внешних информационных систем;

− определение системных учетных записей, используемых в рамках взаимодействия с информационными системами сторонних организаций осуществляет Администратор ИСПДн в соответствии с документом ООО «Клиника Доктор КИТ».

Инструкция администратора информационной системы персональных данных».

Порядок обработки, хранения и передачи информации с использованием внешних нформационных систем в части передачи и (или) поручения ПДн третьимлицам определяет Ответственный за организацию обработки ПДн в соответствии с документом ООО «Клиника Доктор КИТ» Инструкция лица, ответственного за организацию обработки персональных данных».

Порядок обработки, хранения и передачи информации с использованием внешних информационных систем, в части обеспечения технологического процесса обработки информации, определяется при разработке (модернизации) ИСПДн и приводится в технической и эксплуатационной документации на ИСПДн.

3.2.13 Обеспечение доверенной загрузки средств вычислительной техники (УПД.17)

В ИСПДн ООО «Клиника Доктор КИТ» обеспечивается исключение несанкционированного доступа к программным и (или) техническим ресурсам средств вычислительной техники ИСПДн на этапе его загрузки.

Доверенная загрузка обеспечивает:

− блокирование попыток несанкционированной загрузки нештатной операционной системы (среды) или недоступность информационных ресурсов для чтения или модификации в случае загрузки нештатной операционной системы;

− контроль доступа пользователей к процессу загрузки операционной системы;

− контроль целостности программного обеспечения и аппаратных компонентов

средств вычислительной техники .Обеспечение доверенной загрузки средств вычислительной техники в ИСПДн осуществляется:

− средствами защиты информации в соответствии с техническими и

эксплуатационными документами на СЗПДн;

− организационными мерами путем предоставления физического доступа к критичным средствам вычислительной техники ИСПДн и СЗПДн только Администраторам ИСПДн и Администраторам СЗПДн.

3.3 Подсистема ограничения программной среды (ОПС) Подсистема ограничения программной среды обеспечивает установку и (или) запуск только разрешенного к использованию в ИСПДн программного обеспечения или исключает возможность установки и (или) запуска запрещенного к использованию в ИСПДн программного обеспечения.

3.3.1 Управление установкой (инсталляцией) компонентов программного обеспечения, в том числе определение компонентов, подлежащих установке, настройка параметров установки компонентов,

контроль за установкой компонентов программного обеспечения (ОПС.2) Администратором ИСПДн реализуются следующие функции по управлению установкой (инсталляцией) компонентов программного обеспечения ИСПДн:

− определение, совместно с Администратором СЗПДн, компонентов программного обеспечения (состава и конфигурации), подлежащих установке в ИСПДн после загрузки операционной системы и согласование его с Ответственным за обеспечение безопасности ПДн;

− настройка параметров установки компонентов программного обеспечения, обеспечивающая исключение установки (если осуществимо) компонентов программного обеспечения, спользование которых не требуется для реализации информационной технологии ИСПДн. Администратором СЗПДн совместно с Администратором ИСПДн осуществляется:

− определение и применение параметров настройки компонентов программного обеспечения, включая программные компоненты средств защиты информации, обеспечивающих реализацию мер защиты информации, а также устранение возможных уязвимостей ИСПДн, приводящих к возникновению угроз безопасности информации;

− формирование эталонных конфигураций программных и программно-аппаратных средств ИСПДн в соответствии с пунктом 3.15.2 настоящего Положения (УКФ.2);

− согласование эталонных конфигураций программных и программно-аппаратных средств ИСПДн с Ответственным за обеспечение безопасности ПДн.

Установка (инсталляция) в ИСПДн программного обеспечения (вида, типа,класса программного обеспечения) и (или) его компонентов осуществляется с учетом перечня программного обеспечения и (или) его компонентов, разрешенных к установке в ООО «Клиника Доктор КИТ» («Перечень программного обеспечения и (или) его компонентов, разрешенных к установке в информационных системах персональных данных»).

Установка (инсталляция) в ИСПДн программного обеспечения и (или) его компонентов должна осуществляться только от имени администратора (учетная запись Администратора ИСПДн) в соответствии с пунктом 3.2.5 настоящего Положения (УПД.5).

Контроль установленного (инсталлированного) в ИСПДн программного обеспечения (состав компонентов, параметры установки, конфигурация компонентов) на предмет соответствия его утвержденному перечню («Перечень программного обеспечения и (или) его компонентов, разрешенных к установке в информационных системах персональных данных») осуществляется

Ответственным за обеспечение безопасности ПДн осуществляется в рамках проводимых регулярных мероприятий по мониторингу и контролю обработки ПДн в соответствии с документом ООО «Клиника Доктор КИТ» . Инструкция лица, ответственного за обеспечение безопасности персональных данных».

3.4 Подсистема защиты машинных носителей персональных данных (ЗНИ)

Подсистема защиты машинных носителей информации, на которых хранятся и обрабатываются ПДн обеспечивает защиту от несанкционированного доступа к машинным носителям и хранящимся на них ПДн, а также несанкционированное использование съемных машинных носителей ПДн.

3.4.1 Учет машинных носителей персональных данных (ЗНИ.1)

В ООО «Клиника Доктор КИТ» учет машинных носителей информации (в том числе носителей ПДн), используемых для хранения и обработки ПДн, осуществляется Администратором СЗПДн путем ведения Журнала учета машинных носителей информации в соответствии с документом ООО «Клиника Доктор КИТ». Руководство администратора системы защиты персональных данных».

Журнал учета машинных носителей информации ведется отдельно для каждой

ИСПДн. Учету подлежат:

− съемные машинные носители информации (флэш-накопители, внешние накопители на жестких дисках и иные устройства);

− портативные вычислительные устройства, имеющие встроенные носители информации (ноутбуки, нетбуки, планшеты, сотовые телефоны, цифровые камеры, звукозаписывающие устройства и иные аналогичные по функциональности устройства);

− машинные носители информации, встроенные в корпус средств вычислительной техники (накопители на жестких дисках).

Учет машинных носителей информации включает присвоение регистрационных (учетных) номеров носителям. В качестве регистрационных номеров используются идентификационные (серийные) номера машинных носителей, присвоенных производителями этих машинных носителей информации, номера инвентарного учета, в том числе инвентарные номера технических средств, имеющих встроенные носители информации, и иные номера.

Учет встроенных в портативные или стационарные технические средства машинных носителей информации может вестись в журналах материально-технического учета в составе соответствующих технических средств. При использовании в составе одного технического средства ИСПДн нескольких встроенных машинных носителей информации, конструктивно объединенных в

единый ресурс для хранения информации, допускается присвоение регистрационного номера техническому средству в целом.

Регистрационные или иные номера подлежат занесению в Журнал учета машинных носителей информации или журналы материально-технического учета с указанием пользователя или группы пользователей, которым разрешен доступ к машинным носителям информации.

Раздельному учету в журналах учета подлежат съемные (в том числе портативные), перезаписываемые машинные носители информации (флэш-накопители, съемные жесткие диски).

Использование в ИСПДн неучтенных машинных носителей информации (в том числе съемных) запрещено.

Контроль выполнения процедур по учету машинных носителей ПДн осуществляется Ответственным за обеспечение безопасности ПДн в рамках проводимых регулярных мероприятий по мониторингу и контролю обработки ПДн в соответствии с документом ООО «Клиника Доктор КИТ» Инструкция лица, ответственного за обеспечение безопасности персональных данных».

3.4.2 Управление доступом к машинным носителям персональных данных (ЗНИ.2)

В ООО «Клиника Доктор КИТ» Ставрополя регламентируется доступ к следующим машинным носителям информации (в том числе носителям ПДн):

− съемные машинные носители информации (флэш-накопители, внешние накопители на жестких дисках и иные устройства);

− портативные вычислительные устройства, имеющие встроенные носители информации (ноутбуки, нетбуки, планшеты, сотовые телефоны, цифровые камеры, звукозаписывающие устройства и иные аналогичные по функциональности устройства);

− машинные носители информации, стационарно устанавливаемые в корпус средств вычислительной техники (например, накопители на жестких дисках). Физический доступ к машинным носителям информации (в том числе носителям ПДн) предоставляется только тем лицам, которым он необходим для выполнения своих должностных обязанностей (функций) в соответствии с пунктом 3.2.5

настоящего Положения (УПД.5).Управление физическим доступом к машинным носителям информации (в том числе носителям ПДн) в ООО «Клиника Доктор КИТ» обеспечивается:

− контролем физического доступа в помещения, в которых осуществляется хранение машинных носителей информации (в том числе с применением систем контроля физического доступа);

− опечатыванием корпуса средства вычислительной техники, в котором стационарно установлен машинный носитель информации.

3.4.3 Уничтожение (стирание) или обезличивание персональных данных на машинных носителях при их передаче между пользователями,

в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) или обезличивания (ЗНИ.8)

В ООО «Клиника Доктор КИТ» Ставрополя уничтожение (стирание) информации на машинных носителях ПДн при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания)

информации осуществляется Администратором СЗПДн в соответствии с документом ООО «Клиника Доктор КИТ» . Руководство администратора системы защиты персональных данных».

При передаче машинных носителей ПДн между пользователями, в сторонние организации для ремонта или утилизации Администратором СЗПДн осуществляется уничтожение (стирание) информации на машинных носителях ПДн, исключающее возможность восстановления защищаемой информации.

Администратором СЗПДн применяются следующие меры по уничтожению (стиранию) информации на машинных носителях ПДн, исключающие возможность восстановления защищаемой информации:

− удаление файлов штатными средствами операционной системы и (или) форматирование машинного носителя информации штатными средствами операционной системы;

− перезапись уничтожаемых (стираемых) файлов случайной битовой последовательностью, удаление записи о файлах, обнуление журнала файловой системы или полная перезапись всего адресного пространства машинного носителя информации случайной битовой последовательностью с последующим форматированием;

− очистка всего физического пространства машинного носителя информации, включая сбойные и резервные элементы памяти специализированными программами или утилитами производителя;

− полная многократная перезапись машинного носителя информации специальными битовыми последовательностями, зависящими от типа накопителя и используемого метода кодирования информации, затем очистка всего физического пространства накопителя, включая сбойные и резервные элементы памяти специализированными программами или утилитами производителя;

− размагничивание машинного носителя информации;

− физическое уничтожение машинных носителей информации (в том числе сжигание, измельчение, плавление, расщепление, распыление и другое), которые не подлежат очистке (неперезаписываемые машинные носители информации, такие как оптические диски типа CD-R).

Уничтожению (стиранию) подлежит информация, хранящаяся на цифровых инецифровых, съемных и несъемных машинных носителях информации (в том числе носителях ПДн).

3.5 Подсистема регистрации событий безопасности (РСБ)

Подсистема регистрации событий безопасности обеспечивает сбор, запись, хранение и защиту информации о событиях безопасности в ИСПДн, а также возможность просмотра и анализа информации о таких событиях и реагирование на них.

3.5.1 Определение событий безопасности, подлежащих регистрации,и сроков их хранения (РСБ.1)

В ООО «Клиника Доктор КИТ» события безопасности, подлежащие регистрации в ИСПДн, определены с учетом способов реализации угроз безопасности для ПДн при их обработке в ИСПДн. К событиям безопасности, подлежащим регистрации в ИСПДн отнесены любые проявления состояния ИСПДн и ее системы защиты информации, указывающие на возможность нарушения

конфиденциальности, целостности или доступности информации, доступности компонентов ИСПДн, нарушения процедур, установленных локальными актами по защите информации в ООО «Клиника Доктор КИТ», а также на нарушение штатного функционирования средств защиты информации.

События безопасности, подлежащие регистрации в ИСПДн, и сроки хранения соответствующих записей регистрационных журналов обеспечивают возможность обнаружения, идентификации и анализа компьютерных инцидентов, возникших в ИСПДн. В ИСПДн подлежат регистрации события безопасности, связанные с применением выбранных мер по защите информации. Перечень событий безопасности, регистрация которых осуществляется в текущий момент времени,определяется Ответственным за обеспечение безопасности ПДн совместно с Администратором СЗПДн и Администратором ИСПДн исходя из возможностей реализации угроз безопасности информации.

В ООО «Клиника Доктор КИТ» . Ставрополя как минимум подлежат регистрации следующие события:

− вход (выход), а также попытки входа субъектов доступа в ИСПДн и загрузки (останова) операционной системы;

− подключение машинных носителей информации и вывод информации на носители информации;

− запуск (завершение) программ и процессов (заданий, задач), связанных собработкой защищаемой информации;

− попытки доступа программных средств к определяемым ООО «Клиника Доктор КИТ» защищаемым объектам доступа (техническим средствам, узлам сети, линиям (каналам) связи, внешним устройствам, программам, томам,каталогам, файлам, записям, полям записей) и иным объектам доступа;

− попытки удаленного доступа.Состав и содержание информации о событиях безопасности, подлежащих регистрации в ИСПДн определяется в соответствии с пунктом 3.5.2 настоящего

Положения (РСБ.2).

В ИСПДн ГБУЗ СК «ГККДП» г. Ставрополя обеспечивается:

− пересмотр перечня событий безопасности, подлежащих регистрации, неменее чем один раз в год, а также по результатам контроля (мониторинга) заобеспечением уровня защищенности информации, содержащейся в ИСПДн;

− включение в перечень событий безопасности, подлежащих регистрации, событий, связанных с действиями от имени привилегированных учетных записей (администраторов);

− включение в перечень событий безопасности, подлежащих регистрации, событий, связанных с изменением привилегий учетных записей;

− срок хранения информации о зарегистрированных событиях безопасности не менее трех месяцев, если иное не установлено требованиями законодательства Российской Федерации, при этом осуществляется хранение только записей о выявленных событиях безопасности.

3.5.2 Определение состава и содержания информации о событиях безопасности, подлежащих регистрации (РСБ.2)

В ИСПДн ООО «Клиника Доктор КИТ» осуществляется запись информации о событиях безопасности, включающая:

− тип события безопасности;

− дату и время события безопасности;

− идентификационная информация источника события безопасности;

− результат события безопасности (успешно или неуспешно);

− субъект доступа (пользователь и (или) процесс), связанный с данным событием безопасности;

− полнотекстовую запись привилегированных команд (команд, управляющих системными функциями);

− и иную информацию.

В ООО «Клиника Доктор КИТ»осуществляется запись информации при регистрации входа (выхода) субъектов доступа в ИСПДн и загрузки (останова) операционной системы включающая:

− дату и время входа (выхода) в систему (из системы) или загрузки (останова) операционной системы;

− результат попытки входа (успешная или неуспешная);

− результат попытки загрузки (останова) операционной системы (успешная или неуспешная);

− идентификатор, предъявленный при попытке доступа.

В ИСПДн ООО «Клиника Доктор КИТ» осуществляется запись информации при регистрации подключения машинных носителей информации и вывода информации на носители информации включающая:

− дату и время подключения машинных носителей информации и вывода информации на носители информации;

− логическое имя (номер) подключаемого машинного носителя информации;

− идентификатор субъекта доступа, осуществляющего вывод информации на носитель информации.

В ООО «Клиника Доктор КИТ» осуществляется запись информации при регистрации запуска (завершения) программ и процессов (заданий, задач),

связанных с обработкой защищаемой информации включающая:

− дату и время запуска;

− имя (идентификатор) программы (процесса, задания);

− идентификатор субъекта доступа (устройства), запросившего программу (процесс, задание);

− результат запуска (успешный, неуспешный).

В ООО «Клиника Доктор КИТ» осуществляется запись информации при регистрации попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам включающая:

− дату и время попытки доступа к защищаемому файлу с указанием ее результата (успешная, неуспешная);

− идентификатор субъекта доступа (устройства), спецификацию защищаемого файла (логическое имя, тип).

В ООО «Клиника Доктор КИТ» осуществляется запись информации при регистрации попыток доступа программных средств к защищаемым объектам доступа (техническим средствам, узлам сети, линиям (каналам) связи, внешним устройствам, программам, томам, каталогам, записям, полям записей) включающая:

− дату и время попытки доступа к защищаемому объекту с указанием ее результата (успешная, неуспешная);

− идентификатор субъекта доступа (устройства);

− спецификацию защищаемого объекта доступа (логическое имя (номер).

В ООО «Клиника Доктор КИТ» осуществляется запись информации при регистрации попыток удаленного доступа к информационной системе включающая:

− дату и время попытки удаленного доступа с указанием ее результата (успешная, неуспешная);

− идентификатор субъекта доступа (устройства);

− используемый протокол доступа;

− используемый интерфейс доступа и (или) иную информацию о попытках удаленного доступа к информационной системе.

3.5.3 Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения (РСБ.3)

В ООО «Клиника Доктор КИТ» сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения предусматривает:

− возможность выбора Администратором СЗПДн событий безопасности, подлежащих регистрации в текущий момент времени осуществляется из перечня событий безопасности, определенных в соответствии с пунктом 3.5.1 настоящего Положения (РСБ.1);

− генерацию (сбор, запись) записей регистрации (аудита) для событий безопасности, подлежащих регистрации (аудиту) в соответствии с пунктом 3.5.1 настоящего Положения (РСБ.1) с составом и содержанием информации, определенными в соответствии с пунктом 3.5.2 настоящего Положения

(РСБ.2);

− хранение информации о событиях безопасности в течение времени, установленного в соответствии с пунктом 3.5.1 настоящего Положения (РСБ.1).

Объем памяти для хранения информации о событиях безопасности должен быть рассчитан и выделен с учетом типов событий безопасности, подлежащих регистрации в соответствии с пунктом 3.5.1 настоящего Положения (РСБ.1), составом и содержанием информации о событиях безопасности, подлежащих регистрации, в соответствии с пунктом 3.5.2 настоящего Положения (РСБ.2), прогнозируемой частоты возникновения подлежащих регистрации событий безопасности, срока хранения информации о зарегистрированных событиях безопасности в соответствии с пунктом 3.5.1 настоящего Положения (РСБ.1).

3.5.4 Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них (РСБ.5)

Мониторинг (просмотр и анализ) записей регистрации (аудита) событий безопасности осуществляется для всех событий, подлежащих регистрации в соответствии с пунктом 3.5.1 настоящего Положения (РСБ.1), с установленной периодичностью обеспечивающей своевременное выявление признаков инцидентов безопасности в ООО «Клиника Доктор КИТ».

Выявление признаков компьютерных инцидентов безопасности в ООО «Клиника Доктор КИТ»

проведение мероприятий по реагированию на выявленные компьютерные инциденты и принятие мер по устранению последствий компьютерных инцидентов осуществляется в соответствии с пунктом 3.14 настоящего Положения (ИНЦ.1 – ИНЦ.6).

3.5.5 Защита информации о событиях безопасности (РСБ.7)

Защита информации о событиях безопасности (записях регистрации (аудита)) осуществляется применением мер защиты информации, определенных в соответствии с настоящим Положением, и включает защиту средств регистрации (аудита) событий безопасности и настроек механизмов регистрации событий. Доступ к записям аудита и функциям управления механизмами регистрации

(аудита) предоставляется в соответствии с пунктом 3.2.5 настоящего Положения(УПД.5).

3.6 Подсистема антивирусной защиты (АВЗ)

Подсистема антивирусной защиты обеспечивает обнаружение в ООО «Клиника Доктор КИТ» компьютерных программ либо иной компьютерной информации, предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средствами защиты информации, а также реагирование на обнаружение этих программ и информации.

3.6.1 Реализация антивирусной защиты (АВЗ.1)

В ООО «Клиника Доктор КИТ» антивирусная защита ИСПДн, включающая обнаружение компьютерных программ либо иной компьютерной информации, предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирование на

обнаружение этих программ и информации осуществляется с использованием средств антивирусной защиты в соответствии с техническими и эксплуатационными документами ООО «Клиника Доктор КИТ».

Реализация антивирусной защиты предусматривает:

− применение средств антивирусной защиты в соответствии с техническими и эксплуатационными документами ООО «Клиника Доктор КИТ»;

− проведение антивирусного контроля;

− восстановления информации и работоспособности средств вычислительной техники в случае реализованного вирусного воздействия.

Антивирусный контроль осуществляется:

− на плановой основе:

о при загрузке операционной системы автоматизированных рабочих мест и серверов ИСПДн;

о в загруженной операционной системе автоматизированных рабочих мест не реже 1 (одного) раза в неделю (полное сканирования всех машинных носителей информации постоянно установленных либо съемных);

о в загруженной операционной системе серверов ИСПДн не реже 1 (одного) раза в 30 (тридцать) дней;

о в электронных архивах не реже 1 (одного) раза в месяц;

− внепланово:

о для любой информации (текстовых файлов любых форматов, файлов

данных, исполняемых файлов), получаемой и передаваемой по телекоммуникационным каналам;

о при подключении съемных носителей информации к техническим средствам, входящим в состав ИСПДн для любой информации (текстовых файлов любых форматов, файлов данных, исполняемых файлов) на съёмных носителях (магнитные диски, ленты, оптические диски, USB-диски и т.п.), получаемой от сторонних лиц и организаций для файлов, помещаемых в электронный архив;

о после установки (модификации) программного обеспечения технических средств, входящих в состав ИСПДн; о при возникновении подозрения на наличие компьютерного вируса.

В случае обнаружения вредоносной компьютерной программы (вируса),инфицированного файла в рамках антивирусного контроля выполняются следующие действия:

− лечение (очистка) файла от обнаруженного вируса с предварительным созданием резервной копии;

− при невозможности удаления тела вируса из файла или обнаружении «троянской программы», «сетевого червя» и т.п. данный объект перемещается в специально выделенную закрытую

директорию (карантинную зону);− оповещение Администратора СЗПДн о результатах указанных выше операций.

Обязанности Ответственного за обеспечений безопасности ПДн, Администратора СЗПДн, Администратора ИСПДн и Пользователей ИСПДн в части обеспечения антивирусной защиты определены в соответствующих документах:

− ООО «Клиника Доктор КИТ» ответственного за обеспечение безопасности персональных данных»;

−ООО «Клиника Доктор КИТ»

. Руководство администратора системы защиты персональных данных»;

−ООО «Клиника Доктор КИТ»

. Инструкция администратора информационной системы персональных данных»;

− ООО «Клиника Доктор КИТ». Инструкция пользователя информационной системы персональных данных».

3.6.2 Обновление базы данных признаков вредоносных компьютерных программ (вирусов) (АВЗ.2)

Обновление базы данных признаков вредоносных компьютерных программ (вирусов) осуществляется Администратором СЗПДн в соответствии с документом ООО «Клиника Доктор КИТ» Руководство администратора системы защиты персональных данных», техническими и эксплуатационными документами ООО «Клиника Доктор КИТ» а также эксплуатационной документацией средств антивирусной защиты. Обновление базы данных признаков вредоносных компьютерных программ(вирусов) предусматривает:

− получение уведомлений о необходимости обновлений и непосредственном обновлении базы данных признаков вредоносных компьютерных программ (вирусов);

− получение из доверенных источников и установку обновлений базы данных признаков вредоносных компьютерных программ (вирусов);

− контроль целостности обновлений базы данных признаков вредоносных компьютерных программ (вирусов).

3.7 Подсистема обнаружения вторжений (СОВ)

Подсистема обнаружения вторжений обеспечивает обнаружение действий в ООО «Клиника Доктор КИТ», направленных на несанкционированный доступ к информации, специальные воздействия на ИСПДн и (или) ПДн в целях их добывания, уничтожения, искажения и блокирования доступа к ПДн, а также реагирование на эти действия.

3.7.1 Обнаружение вторжений (СОВ.1)

Обнаружение (предотвращение) вторжений (компьютерных атак), направленных на преднамеренный несанкционированный доступ к информации, специальные воздействия на информацию (носители информации) в целях ее добывания, уничтожения, искажения и

блокирования доступа к ней, осуществляется с использованием систем обнаружения вторжений в соответствии с техническими и эксплуатационными документами СЗПДн ООО «Клиника Доктор КИТ».

3.7.2 Обновление базы решающих правил (СОВ.2)

Обновление базы решающих правил системы обнаружения вторжений осуществляется Администратором СЗПДн в соответствии с документом ООО «Клиника Доктор КИТ». Руководство администратора системы защиты персональных данных», техническими и эксплуатационными документами СЗПДн ООО «Клиника Доктор КИТ», а также эксплуатационной документацией системы обнаружения вторжений.

Обновление базы решающих правил системы обнаружения вторжений предусматривает:

− получение уведомлений о необходимости обновлений и непосредственном обновлении базы решающих правил;

− получение из доверенных источников и установку обновлений базы решающих правил;

− контроль целостности обновлений базы решающих правил.

3.8 Подсистема контроля (анализа) защищенности персональных данных (АНЗ)

Подсистема контроля (анализа) защищенности ПДн обеспечивает контроль уровня защищенности ПДн, обрабатываемых в ИСПДн ООО «Клиника Доктор КИТ», путем проведения систематических мероприятий по анализу защищенности информационной системы и тестированию работоспособности СЗПДн.

3.8.1 Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей (АНЗ.1)

При выявлении (поиске), анализе и устранении уязвимостей в ИСПДн ООО «Клиника Доктор КИТ» Администратором СЗПДн осуществляется:

− выявление (поиск) уязвимостей, связанных с ошибками кода в программном (микропрограммном) обеспечении (общесистемном, прикладном, специальном), а также программном обеспечении средств защиты информации, правильностью установки и настройки средств защиты информации, технических средств и программного обеспечения, а также корректностью работы средств защиты информации при их взаимодействии с техническими средствами и программным обеспечением;

− использование для выявления (поиска) уязвимостей средств анализа (контроля) защищенности (сканеров безопасности), имеющих стандартизованные (унифицированные) в соответствии с национальными стандартами описание и перечни программно-аппаратных платформ, уязвимостей программного обеспечения, ошибочных конфигураций, правил описания уязвимостей, проверочных списков, процедур тестирования и языка тестирования ИСПДн на наличие уязвимостей, оценки последствий уязвимостей, имеющих возможность оперативного обновления базы данных выявляемых уязвимостей;

− анализ журналов регистрации событий безопасности (журнала аудита) в целях определения, были ли выявленные уязвимости ранее использованы в ИСПДн для нарушения безопасности информации;

− тестирование на проникновение в условиях, соответствующих возможностям нарушителей, определенных при моделировании угроз безопасности информации;

− предоставление Ответственному за обеспечение безопасности ПДн Отчетов с описанием выявленных уязвимостей и планом мероприятий по их устранению.

В качестве источников информации об уязвимостях используются опубликованные данные разработчиков средств защиты информации, общесистемного, прикладного и специального программного обеспечения,технических средств, а также другие базы данных уязвимостей.

При анализе и устранении уязвимостей Ответственный за обеспечение безопасности СЗПДн осуществляет:

− анализ Отчетов Администратора СЗПДн по результатам выявления (поиска) уязвимостей и оценку достаточности реализованных мер защиты информации;

− анализ изменения угроз безопасности информации в ИСПДн, возникающих в ходе его эксплуатации, и оценка возможных последствий реализации угроз безопасности информации в ИСПДн;

− включение мероприятий по устранению уязвимостей в план мероприятий по обеспечению безопасности ИСПДн;

− обеспечение устранения выявленных уязвимостей, в том числе путем установки обновлений программного обеспечения средств защиты информации, общесистемного программного обеспечения, прикладного программного обеспечения или микропрограммного обеспечения технических средств Администратором СЗПДн или Администратором ИСПДн;

− информирование пользователей ИСПДн, Администраторов ИСПДн, Администраторов СЗПДн о результатах поиска уязвимостей и оценки достаточности реализованных мер защиты информации.

Поиск и анализ уязвимостей проводится с установленной периодичностью в зависимости от особенностей функционирования ИСПДн. При этом в обязательном порядке для критических уязвимостей проводится поиск и анализ уязвимостей в случае опубликования в общедоступных источниках информации о новых уязвимостях в средствах защиты информации, технических средствах и программном обеспечении, применяемом в ИСПДн.

В случае невозможности устранения выявленных уязвимостей путем установки обновлений программного обеспечения средств защиты информации, общесистемного программного обеспечения, прикладного программного обеспечения или микропрограммного обеспечения технических средств необходимо предпринять действия (настройки средств защиты информации, изменение режима и порядка использования ИСПДн), направленные на устранение возможности использования выявленных уязвимостей.

3.8.2 Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации (АНЗ.2)

В ООО «Клиника Доктор КИТ» осуществляется получение из доверенных источников и установка обновлений программного обеспечения, включая программное обеспечение средств защиты информации и программное обеспечение базовой системы ввода-вывода.

При контроле установки обновлений осуществляется проверка соответствия версий бщесистемного, прикладного и специального программного (микропрограммного) обеспечения, включая программное обеспечение средств защиты информации, установленного в ИСПДн и выпущенного разработчиком, а также наличие отметок в эксплуатационной документации (формуляр или паспорт) об установке (применении) обновлений.

Контроль установки обновлений в ИСПДн проводится с установленной периодичностью в зависимости от особенностей функционирования ИСПДн и фиксируется в соответствующих журналах.

При контроле установки обновлений осуществляются проверки установки обновлений баз данных признаков вредоносных компьютерных программ (вирусов)

средств антивирусной защиты в соответствии с пунктом 3.6.2 настоящего Положения (АВЗ.2), баз решающих правил систем обнаружения вторжений в соответствии с пунктом 3.7.2 настоящего Положения (СОВ.2), баз признаков уязвимостей средств анализа защищенности и иных баз данных, необходимых для реализации функций безопасности средств защиты информации.

3.8.3 Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации (АНЗ.3)

При контроле работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации в ИСПДн ООО «Клиника Доктор КИТ» осуществляется:

− контроль работоспособности (неотключения) программного обеспечения и

средств защиты информации;

− проверка правильности функционирования (тестирование на тестовых данных, приводящих к известному результату) программного обеспечения и средств защиты информации;

− контроль соответствия настроек программного обеспечения и средств защиты информации параметрам настройки, приведенным в эксплуатационной документации на СЗПДн и средства защиты информации;

− регистрация событий и оповещение (сигнализация, индикация)

Администратора СЗПДн о событиях, связанных с нарушением работоспособности (правильности функционирования) и параметров настройки программного обеспечения и средств защиты информации;

− восстановление работоспособности (правильности функционирования) и параметров настройки программного обеспечения и средств защиты информации (при необходимости), в том числе с использованием резервных копий и (или) дистрибутивов.

Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации проводится с установленной периодичностью в зависимости от особенностей функционирования ИСПДн и фиксируется в соответствующих журналах.

3.8.4 Контроль состава технических средств, программного обеспечения и средств защиты информации (АНЗ.4)

При контроле состава технических средств, программного обеспечения и средств защиты информации в ИСПДн ООО «Клиника Доктор КИТ» осуществляется:

− контроль соответствия состава технических средств, программного обеспечения и средств защиты информации приведенному в эксплуатационной документации с целью поддержания актуальной

(установленной в соответствии с эксплуатационной документацией) конфигурации ИСПДн и принятие мер, направленных на устранение выявленных недостатков;

− контроль состава технических средств, программного обеспечения и средств защиты информации на соответствие сведениям действующей (актуализированной) эксплуатационной документации и принятие мер,направленных на устранение выявленных недостатков;

− контроль выполнения условий и сроков действия сертификатов соответствия на средства защиты информации и принятие мер, направленных на устранение выявленных недостатков;

− исключение (восстановление) из состава ИСПДн несанкционированно установленных (удаленных) технических средств, программного обеспечения и средств защиты информации.

3.8.5 Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступа, полномочий пользователей в

информационной системе (АНЗ.5)

При контроле правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в ИСПДн ООО «Клиника Доктор КИТ» осуществляется:

− контроль правил генерации и смены паролей пользователей в соответствии с

пунктами 3.1.1, 3.1.4 настоящего Положения (ИАФ.1, ИАФ.4);

− контроль заведения и удаления учетных записей пользователей в соответствии с пунктом 3.2.1 настоящего Положения (УПД.1);

− контроль реализации правил разграничения доступом в соответствии с пунктом 3.2.2 настоящего Положения (УПД.2);

− контроль реализации полномочий пользователей в соответствии с пунктами 3.2.4, 3.2.5 настоящего Положения (УПД.4, УПД.5);

− контроль наличия документов, подтверждающих разрешение изменений учетных записей пользователей, их параметров, правил разграничения доступом и полномочий пользователей,

предусмотренных организационно-распорядительными документами по защите информации ООО «Клиника Доктор КИТ»

− регистрация событий, связанных со сменой паролей пользователей, заведением и удалением учетных записей пользователей, изменением правил разграничения доступом и полномочий пользователей;

− устранение нарушений, связанных с генерацией и сменой паролей пользователей, заведением и удалением учетных записей пользователей, реализацией правил разграничения доступом, установлением полномочий пользователей.

3.9 Подсистема обеспечения целостности информационной системы и персональных данных (ОЦЛ)

Подсистема обеспечения целостности ИСПДн и ПДн обеспечивает обнаружение фактов несанкционированного нарушения целостности ИСПДн и содержащихся в ней ПДн, а также возможность восстановления ИСПДн и содержащихся в них ПДн.

3.9.1 Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации (ОЦЛ.1)

В ИСПДн ООО «Клиника Доктор КИТ» осуществляется контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации.

Контроль целостности программного обеспечения ИСПДн осуществляется Администратором СЗПДн и Администратором ИСПДн и предусматривает:

− контроль целостности компонентов программного по наличию имен (идентификаторов) компонентов программного обеспечения и (или) по контрольным суммам в процессе загрузки и (или) динамически в процессе работы ИСПДн;

− контроль применения средств разработки и отладки программ в составе программного обеспечения ИСПДн.

Контроль целостности программного обеспечения средств защиты информации ИСПДн осуществляется Администратором СЗПДн и предусматривает:

− тестирование функций безопасности средств защиты информации, в том числе с помощью тест-программ, имитирующих попытки несанкционированного доступа, и (или) специальных программных средств, в соответствии с пунктами 3.8.1, 3.8.2 настоящего Положения (АНЗ.1, АНЗ.2);

− контроль целостности программного обеспечения средств защиты информации, включая их обновления, по наличию имен (идентификаторов) и (или) по контрольным суммам компонентов средств защиты информации в процессе загрузки и (или) динамически в процессе работы ИСПДн;

− организация обеспечения физической защиты технических средств ИСПДн в соответствии с пунктом 3.12.1 настоящего Положения (ЗТС.3).

В случае, если функциональные возможности ИСПДн должны предусматривать применение в составе ее программного обеспечения средств разработки и отладки программ, Администратором ИСПДн обеспечивается выполнение процедур контроля целостности программного обеспечения после завершения каждого процесса функционирования средств разработки и отладки программ.

3.9.2 Обнаружение и реагирование на поступление в информационную систему незапрашиваемых электронных сообщений (писем, документов) и иной информации, не относящихся к функционированию информационной системы (защита от спама) (ОЦЛ.4)

Защита от спама реализуется на точках входа (выхода) в ИСПДн ООО «Клиника Доктор КИТ» информационных потоков (межсетевые экраны, почтовые серверы, Web-серверы, прокси-серверы и серверы удаленного доступа), а также на автоматизированных рабочих местах, серверах и (или) мобильных технических средствах, подключенных к сетям связи общего пользования, для обнаружения и реагирования на поступление по электронной почте незапрашиваемых электронных

сообщений (писем, документов) или в приложениях к электронным письмам. Защита от спама в ИСПДн обеспечивается применением специализированных средств защиты, реализующих следующие механизмы защиты:

− фильтрация по содержимому электронных сообщений (писем, документов) с использованием критериев, позволяющих относить сообщения к спаму сигнатурным и (или) эвристическим методами;

− фильтрация на основе информации об отправителе электронного сообщения (в том числе с использованием создания «черных»" списков (запрещенные отправители) и (или) «белых» списков (разрешенные отправители).

3.10 Подсистема обеспечения доступности персональных данных (ОДТ)

Подсистема обеспечения доступности ПДн обеспечивает авторизованный доступ пользователей, имеющих права по доступу, к ПДн, содержащимся в ИСПДн, в штатном режиме функционирования ИСПДн.

3.10.1 Периодическое резервное копирование персональных данных на резервные машинные носители персональных данных (ОДТ.4)

В ООО «Клиника Доктор КИТ» Администратором СЗПДн и Администратором ИСПДн осуществляется периодическое резервное копирование информации на резервные машинные носители информации, предусматривающее:

− разработку перечня информации (типов информации), подлежащей периодическому резервному копированию на резервные машинные носители информации;

− резервное копирование информации на резервные машинные носители информации с установленной оператором периодичностью в зависимости от особенностей функционирования ИСПДн;

− регистрацию событий, связанных с резервным копированием информации на резервные машинные носители информации;

− принятие мер для защиты резервируемой информации, обеспечивающих ее конфиденциальность, целостность и доступность в соответствии с настоящим Положением;

− проверка работоспособности средств резервного копирования, средств хранения резервных копий и средств восстановления информации из резервных копий.

3.10.2 Обеспечение возможности восстановления персональных данных с резервных машинных носителей персональных данных (резервных копий) в течение установленного временного интервала (ОДТ.5)

В ИСПДн ООО «Клиника Доктор КИТ» и Администратором ИСПДн обеспечивается возможность восстановления информации с резервных машинных носителей информации (резервных копий).

Восстановление информации с резервных машинных носителей информации (резервных копий) предусматривает:

− восстановление информации с резервных машинных носителей информации (резервных копий) в зависимости от особенностей функционирования ИСПДн;

− регистрация событий, связанных восстановлением информации с резервных машинных носителей информации;

− определение времени, в течение которого должно быть обеспечено восстановление информации и обеспечивающего требуемые условия непрерывности функционирования ИСПДн и доступности информации;

− периодическую проверку возможности восстановления информации с резервных машинных носителей информации в соответствии с пунктом 3.10.1 настоящего Положения (ОДТ.4).

3.11 Подсистема защиты среды виртуализации (ЗСВ) Подсистема защиты среды виртуализации обеспечивает защиту от несанкционированного доступа к ПДн, обрабатываемым в виртуальной

инфраструктуре, и к компонентам виртуальной инфраструктуры и (или) воздействия на них, 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, а также системе резервного копирования и создаваемым ею копиям.

3.11.1 Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации (ЗСВ.1)

В ИСПДн ООО «Клиника Доктор КИТ» обеспечивается идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе

администраторов управления средствами виртуализации, в соответствии с пунктами 3.1.1 – 3.1.6 настоящего Положения (ИАФ.1– ИАФ.6).

При реализации мер по идентификации и аутентификации субъектов доступа и объектов доступа в виртуальной инфраструктуре обеспечивается:

− идентификация и аутентификация администраторов управления средствами виртуализации;

− идентификация и аутентификация субъектов доступа при их локальном и удаленном обращении к объектам доступа в виртуальной инфраструктуре;

− блокировка доступа к компонентам виртуальной инфраструктуры для субъектов доступа, не прошедших процедуру аутентификации;

− защита аутентификационной информации субъектов доступа, хранящейся в компонентах виртуальной инфраструктуры от неправомерных доступа к ней уничтожения или модифицирования;

− защита аутентификационной информации в процессе ее ввода для аутентификации в виртуальной инфраструктуре от возможного использования лицами, не имеющими на это полномочий;

− взаимная идентификация и аутентификация пользователя и сервера виртуализации (виртуальных машин) при удаленном доступе;

− идентификация и аутентификация субъектов доступа при осуществлении ими попыток доступа к средствам управления параметрами аппаратного обеспечения виртуальной инфраструктуры.

Внутри развернутых на базе виртуальной инфраструктуры виртуальных машин реализация мер по идентификации и аутентификации субъектов и объектов доступа осуществляется в соответствии с пунктами 3.1.1 – 3.1.6 настоящего Положения (ИАФ.1 – ИАФ.6).

3.11.2 Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин (ЗСВ.2)

В ИСПДн ООО «Клиника Доктор КИТ» обеспечивается управление доступом субъектов доступа к объектам доступа, в том числе внутри виртуальных машин, в соответствии с пунктами 3.2.1, 3.2.2, 3.2.4 –3.2.6, 3.2.7 –3.2.9 настоящего Положения (УПД.1, УПД.2, УПД.4 – УПД.6, УПД.10 – УПД.13). При реализации мер по управлению доступом субъектов доступа к объектам

доступа в виртуальной инфраструктуре обеспечивается:

− контроль доступа субъектов доступа к средствам управления компонентами виртуальной инфраструктуры;

− контроль доступа субъектов доступа к файлам-образам виртуализированного программного обеспечения, виртуальных машин, файлам-образам, служебным данным, используемым для обеспечения работы виртуальных файловых систем, и иным служебным данным средств виртуальной среды;

− управление доступом к виртуальному аппаратному обеспечению ИСПДн,

являющимся объектом доступа;

− контроль запуска виртуальных машин на основе заданных оператором правил (режима запуска, типа используемого носителя и иных правил).

Дополнительно при управлении доступом субъектов доступа к объектам доступа обеспечивается:

− разграничение доступа субъектов доступа, зарегистрированных на виртуальных машинах, к объектам доступа, расположенным внутри виртуальных машин, в соответствии с правилами разграничения доступа пользователей данных виртуальных машин (потребителей облачных услуг);

− разграничение доступа субъектов доступа, зарегистрированных на виртуальных машинах, к ресурсам ИСПДн, размещенным за пределами виртуальных машин, в соответствии с правилами разграничения доступа,принятыми в ИСПДн в целом.

3.11.3 Регистрация событий безопасности в виртуальной инфраструктуре (ЗСВ.3)

В ИСПДн ООО «Клиника Доктор КИТ» обеспечивается регистрация событий безопасности в виртуальной инфраструктуре в соответствии с пунктами 3.5.1 –3.5.3,3.5.4 настоящего Положения (РСБ.1 – РСБ.3, РСБ.5).

При реализации мер по регистрации событий безопасности в виртуальной инфраструктуре дополнительно к событиям, установленным в пункте 3.5.1настоящего Положения (РСБ.1), регистрируются следующие события:

− запуск (завершение) работы компонентов виртуальной инфраструктуры;

− доступ субъектов доступа к компонентам виртуальной инфраструктуры;

− изменения в составе и конфигурации компонентов виртуальной инфраструктуры во время их запуска, функционирования и аппаратного отключения;

− изменения правил разграничения доступа к компонентам виртуальной инфраструктуры.

При регистрации запуска (завершения) работы компонентов виртуальной инфраструктуры состав и содержание информации, подлежащей регистрации, включает:

− дату и время запуска (завершения) работы гипервизора и виртуальных машин, хостостовой операционной системы, программ и процессов в виртуальных машинах;

− результат запуска (завершения) работы указанных компонентов виртуальной инфраструктуры (успешная или неуспешная);

− идентификатор пользователя, предъявленный при попытке запуска (завершения) работы указанных компонентов виртуальной инфраструктуры.

При регистрации входа (выхода) субъектов доступа в компоненты виртуальной инфраструктуры состав и содержание информации, подлежащей регистрации включает:

− дату и время доступа субъектов доступа к гипервизору и виртуальной машине к хостовой операционной системе;

− результат попытки доступа субъектов доступа к указанным компонентам виртуальной инфраструктуры (успешная или неуспешная);

− идентификатор пользователя, предъявленный при попытке доступа субъектов доступа к указанным компонентам виртуальной инфраструктуры.

При изменении в составе и конфигурации компонентов виртуальной инфраструктуры во время запуска, функционирования и в период ее аппаратного отключения состав и содержание информации, подлежащей регистрации, включает:

− дату и время изменения в составе и конфигурации виртуальных машин виртуального аппаратного обеспечения, виртуализированного программного обеспечения, виртуального аппаратного обеспечения в гипервизоре и в виртуальных машинах, в хостовой операционной системе, виртуальном сетевом оборудовании;

− результат попытки изменения в составе и конфигурации указанных компонентов виртуальной инфраструктуры (успешная или неуспешная);

− идентификатор пользователя, предъявленный при попытке изменения в составе и конфигурации указанных компонентов виртуальной инфраструктуры.

При изменении правил разграничения доступа к компонентам виртуальной инфраструктуры состав и содержание информации, подлежащей регистрации включает:

− дату и время изменения правил разграничения доступа к виртуальному и физическому аппаратному обеспечению, к файлам-образам виртуализированного программного обеспечения и виртуальных машин, к файлам-образам, используемым для обеспечения работы виртуальных файловых систем, к виртуальному сетевому оборудованию, к защищаемой информации, хранимой и обрабатываемой в гипервизоре и виртуальных машинах, в хостовой операционной системе;

− результат попытки изменения правил разграничения доступа к указанным компонентам виртуальной инфраструктуры (успешная или неуспешная);

− идентификатор пользователя, предъявленный при попытке изменения правил разграничения доступа к указанным компонентам виртуальной инфраструктуры.

3.11.4 Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных (ЗСВ.6)

В ООО «Клиника Доктор КИТ» обеспечивается управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных.

При управлении перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных обеспечивается:

− регламентирование порядка перемещения (определение ответственных за организацию процесса, объектов перемещения, ресурсов инфраструктуры, задействованных в перемещении, а также способов перемещения);

− управление размещением и перемещением файлов-образов виртуальных машин (контейнеров) между носителями (системами хранения данных);

− управление размещением и перемещением исполняемых виртуальных машин (контейнеров) между серверами виртуализации;

− управление размещением и перемещением данных, обрабатываемых с использованием виртуальных машин, между носителями (системами хранения данных);

− перемещение виртуальных машин (контейнеров) и обрабатываемых на них данных в пределах ИСПДн только на контролируемые им (или уполномоченным лицом) технические средства (сервера виртуализации, носители, системы хранения данных).

Управление перемещением виртуальных машин (контейнеров) предусматривает:

− полный запрет перемещения виртуальных машин (контейнеров);

− ограничение перемещения виртуальных машин (контейнеров) в пределах ИСПДн (сегмента ИСПДн);

− ограничение перемещения виртуальных машин (контейнеров) между сегментами ИСПДн.

3.11.5 Контроль целостности виртуальной инфраструктуры и ее конфигураций (ЗСВ.7)

В ИСПДн ООО «Клиника Доктор КИТ» осуществляется контроль целостности компонентов виртуальной инфраструктуры в соответствии с пунктом 3.9.1 настоящего Положения (ОЦЛ.1).

При реализации мер по контролю целостности компонентов виртуальной инфраструктуры должны обеспечиваться:

− контроль целостности компонентов, критически важных для функционирования хостовой операционной системы, гипервизора, гостевых операционных систем и (или) обеспечения безопасности обрабатываемой в них информации (загрузчика, системных файлов, библиотек операционной системы и иных компонентов);

− контроль целостности состава и конфигурации виртуального оборудования;

− контроль целостности файлов, содержащих параметры настройки виртуализированного программного обеспечения и виртуальных машин;

− контроль целостности файлов-образов виртуализированного программного обеспечения и виртуальных машин, файлов-образов, используемых для обеспечения работы виртуальных файловых систем (контроль файлов- образов должен проводиться во время, когда файлы-образы не

задействованы). В ИСПДн обеспечивается контроль целостности резервных копий виртуальных

машин (контейнеров) в соответствии с пунктом 3.9.1 настоящего Положения (ОЦЛ.1).

В ИСПДн обеспечивается контроль состава аппаратной части компонентов виртуальной инфраструктуры в соответствии с пунктом 3.8.4 настоящего Положения (АНЗ.4).

3.11.6 Резервное копирование данных, резервирование технических средств, программного обеспечения виртуальной инфраструктуры, а также каналов связи внутри виртуальной инфраструктуры (ЗСВ.8) В ИСПДн ООО «Клиника Доктор КИТ» осуществляется резервное

копирование данных, резервирование технических средств, программного обеспечения виртуальной инфраструктуры и каналов связи внутри виртуальной инфраструктуры в соответствии с пунктами 3.10.1, 3.10.2 настоящего Положения (ОДТ.4, ОДТ.5).

При реализации мер по резервному копированию данных, резервированию технических средств, программного обеспечения виртуальной инфраструктуры обеспечивается:

− определение мест хранения резервных копий виртуальных машин (контейнеров) и данных, обрабатываемых в виртуальной инфраструктуре;

− резервное копирование виртуальных машин (контейнеров);

− резервное копирование данных, обрабатываемых в виртуальной инфраструктуре;

− резервирование программного обеспечения виртуальной инфраструктуры;

− резервирование каналов связи, используемых в виртуальной инфраструктуре;

− периодическая проверка резервных копий и возможности восстановления виртуальных машин (контейнеров) и данных, обрабатываемых в виртуальной инфраструктуре с использованием резервных копий.

3.11.7 Реализация и управление антивирусной защитой в виртуальной инфраструктуре (ЗСВ.9)

В ИСПДн ООО «Клиника Доктор КИТ» обеспечивается реализация и управление антивирусной защитой в виртуальной инфраструктуре в соответствии с пунктами 3.6.1, 3.6.2 настоящего Положения (АВЗ.1, АВЗ.2).

При реализации соответствующих мер обеспечивается:

− проверка наличия вредоносных программ (вирусов) в хостовой операционной системе, включая контроль файловой системы, памяти, запущенных приложений и процессов;

− проверка наличия вредоносных программ в гостевой операционной системе в процессе ее функционирования, включая контроль файловой системы, памяти, запущенных приложений и процессов.

3.11.8 Разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки персональных данных отдельным пользователем и (или) группой

пользователей (ЗСВ.10) В ИСПДн ООО «Клиника Доктор КИТ» осуществляется разбиение

виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки информации отдельным пользователем и (или) группой пользователей в соответствии с пунктом 3.13.4 настоящего Положения (ЗИС.17).

3.12 Подсистема защиты технических средств (ЗТС) Подсистема защиты технических средств обеспечивает защиту от несанкционированного доступа к стационарным техническим средствам,

обрабатывающим ПДн, средствам, обеспечивающим функционирование ИСПДн, и в помещения, в которых они постоянно расположены, защиту технических средств от внешних воздействий, а также защиту ПДн, представленных в виде информативных электрических сигналов и физических полей.

3.12.1 Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы, в помещения и сооружения, в которых они установлены (ЗТС.3) Доступ к техническим средствам и средствам защиты информации предоставляется в соответствии с заданными в соответствии с пунктом 2 настоящего Положения ролями в соответствии с пунктом 3.2.5 настоящего Положения (УПД.5).

Контролируемая зона в ООО «Клиника Доктор КИТ» устанавливается приказом руководителя (или иного уполномоченного лица) и включает:

− помещения, здания и территории, на которых осуществляется обработка ПДн (с использованием средств автоматизации или без использования таких средств);

− помещения, здания и территории на которых расположены средства вычислительной техники ИСПДн, СЗПДн и иные технические средства (включая каналы и линии связи), участвующие в обработке ПДн и (или) обеспечивающие функционирование указанных выше средств вычислительной техники.

В контролируемой зоне ООО «Клиника Доктор КИТ» выделены следующие зоны (зоны доступа):

− общедоступная (зона доступ и нахождение лиц, транспортных, технических или иных средств в которой контролируется, но не ограничивается) – помещения, здания и территории с возможностью неограниченного посещения лицам, не являющимися работниками ООО «Клиника Доктор КИТ» (охраняемые территории, открытые для посещений; коридоры и этажи зданий);

− зона доступная для посещения (зона доступ и нахождение лиц, не являющихся работниками ООО «Клиника Доктор КИТ» в которой может осуществляться только в присутствии ответственных работников ООО «Клиника Доктор КИТ» но не ограничивается) – кабинеты и помещения в

которых идет прием населения и (или) оказание услуг населению;

− зона ограниченного посещения (зона доступ и нахождение лиц, не являющихся работниками ООО «Клиника Доктор КИТ» не предусмотрены, но может осуществляться только в сопровождении ответственных работников ООО «Клиника Доктор КИТ» – кабинеты и

помещения не предназначенные для приема населения и (или) оказания услуг населению;

− зона строгого контроля (зона доступ и нахождение лиц, в которой осуществляется строго в соответствии с утвержденным приказом руководителя (или иного уполномоченного

лица) перечнем лиц, имеющих право доступа в указанные зоны доступа) –кабинеты и помещения (в том числе технические) в которых расположены ключевые технические средства ИСПДн и СЗПДн, ключевое сетевое

оборудование, архивы материальных носителей ПДн и т.п.

В пределах установленной контролируемой зоны ООО «Клиника Доктор КИТ» принимаются меры, исключающие неконтролируемое пребывание лиц, не имеющих права доступа (нахождения) в контролируемой зоне, а также исключающие неконтролируемое пребывание в пределах контролируемой зоны транспортных, технических или иных средств.

Доступ в пределы контролируемой зоны предоставляется:

− работникам структурных подразделений ООО «Клиника Доктор КИТ», допущенным к обработке ПДн, в соответствии с приказом руководителя (или иного уполномоченного лица) – на основании утвержденного руководителем ООО «Клиника Доктор КИТ» (или иным уполномоченным лицом) документа ООО «Клиника Доктор КИТ». Перечень лиц, должностей и подразделений, допущенных к обработке персональных данных»;

− лицам, обеспечивающих функционирование (сопровождение, обслуживание,ремонт), управление (администрирование) ИСПДн и СЗПДн ООО «Клиника Доктор КИТ»на основании утвержденного руководителем ООО «Клиника Доктор КИТ» (или иным уполномоченным лицом) перечня лиц,ответственных за внесение изменений в ИСПДн и СЗПДн;

− Ответственный за обеспечение безопасности ПДн).

Доступ в пределы контролируемой зоны (зоны строгого контроля) лиц, не являющихся работниками ООО «Клиника Доктор КИТ», а также лиц, не внесенных в утвержденный приказом руководителя ООО «Клиника Доктор КИТ» (или иного уполномоченного лица) перечень лиц, имеющих право доступа в указанные зоны доступа, осуществляется только в присутствии ответственных работников ООО «Клиника Доктор КИТ» при условии непосредственного сопровождения и контроля пребывания указанных выше лиц ответственным работником ООО «Клиника Доктор КИТ» Доступ в пределы контролируемой зоны (зоны строгого контроля)

регистрируется в Журнале учета посещений соответствующей зоны строгого контроля.

3.12.2 Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр (ЗТС.4)

В ООО «Клиника Доктор КИТ осуществляется размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр.

В качестве устройств вывода (отображения) информации в ИСПДн рассматриваются экраны мониторов автоматизированных рабочих мест пользователей, мониторы консолей управления технических средств (серверов, телекоммуникационного оборудования и иных технических средств), видеопанели, видеостены и другие средства визуального отображения защищаемой информации, печатающие устройства (принтеры, плоттеры и иные устройства), аудиоустройства, многофункциональные устройства.

Размещение устройств вывода (отображения, печати) информации должно исключать возможность несанкционированного просмотра выводимой информации, как из-за пределов контролируемой зоны, так и в пределах контролируемой зоны. Не следует размещать устройства вывода (отображения, печати) информации напротив оконных проемов, входных дверей, технологических отверстий, в коридорах, холлах и иных местах, доступных для несанкционированного просмотра.

В ООО «Клиника Доктор КИТ» . Ставрополя обеспечивается установка на окна помещений ИСПДн средств, ограничивающих возможность визуального ознакомления с защищаемой информацией извне помещений (жалюзи, плотные шторы и иные средства), если в этих помещениях размещены устройства вывода информации на печать и (или) осуществляется отображение информации на видеоустройства.

3.13 Подсистема защиты информационной системы, ее средств, систем связи и передачи данных (ЗИС)

Подсистема защита ИСПДн, ее средств, систем связи и передачи данных обеспечивает защиту ПДн при взаимодействии ИСПДн или ее отдельных сегментов с иными информационными системами и информационно-телекоммуникационными сетями посредством применения архитектуры ИСПДн и проектных решений,направленных на обеспечение безопасности ПДн.

3.13.1 Обеспечение защиты персональных данных от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи (ЗИС.3)

В ООО «Клиника Доктор КИТ» защита ПДн в ИСПДн от раскрытия, модифицирования и навязывания (ввода ложной информации) при их передаче по каналам связи, имеющим выход за пределы контролируемой зоны, обеспечивается путем защиты каналов связи от несанкционированного физического доступа (подключения) к ним и (или) применения в соответствии с законодательством Российской Федерации средств криптографической защиты информации или иными методами в соответствии с техническими и эксплуатационными документами СЗПДн

3.13.2 Обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов (ЗИС.11)

В ИСПДн ООО «Клиника Доктор КИТ» Ставрополя осуществляется обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов (защита от атак типа «человек посередине»).

Подтверждение подлинности сторон сетевого соединения (сеанса взаимодействия) и защиты сетевых устройств и сервисов от подмены осуществляется с помощью их аутентификации в соответствии с пунктом 3.1.2 настоящего Положения (ИАФ.2).

Контроль целостности передаваемой информации включает проверку целостности передаваемых пакетов (в частности, в соответствии с пунктом 3.13.1 настоящего Положения (ЗИС.3)).

3.13.3 Защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки персональных данных (ЗИС.15)

В ИСПДн ООО «Клиника Доктор КИТ» Администратором СЗПДн и Администратором ИСПДн определяются архивные файлы, параметры настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки информации и фиксируются в технических и эксплуатационных документах в соответствии с пунктом 3.15.4

настоящего Положения (УКФ.4).

Защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки информации, обеспечивается принятием мер защиты информации (в частности, в соответствии с пунктами 3.2.2, 3.9.1 настоящего Положения (УПД.2,ОЦЛ.1)). Защита данных, не подлежащих изменению в процессе обработки информации, обеспечивается в отношении информации, хранящейся на жестких магнитных дисках, дисковых накопителях и иных накопителях в ИСПДн.

3.13.4 Разбиение информационной системы на сегменты (сегментирование информационной системы) и обеспечение защиты периметров сегментов информационной системы (ЗИС.17)

В ООО «Клиника Доктор КИТ» осуществляется разбиение ИСПДн на сегменты (сегментирование ИСПДн) с учетом функциональных и технологических особенностей процесса обработки информации и анализа угроз безопасности информации и обеспечивается защита периметров сегментов ИСПДн с целью снижения вероятности реализации угроз и (или) их локализации в рамках одного сегмента.

Принципы сегментирования ИСПДН ООО «Клиника Доктор КИТ» определены и зафиксированы в технических и эксплуатационных документах на СЗПДн. При сегментировании ИСПДн обеспечивается защита периметров сегментов ИСПДн в соответствии с пунктом 3.2.3 настоящего Положения (УПД.3).

3.13.5 Защита беспроводных соединений, применяемых в информационной системе (ЗИС.20)

В ООО «Клиника Доктор КИТ» определены и зафиксированы в технических и эксплуатационных документах на СЗПДн способы и правила обеспечения защиты беспроводных соединений, применяемых в ИСПДн.

Защита беспроводных соединений включает:

− ограничение на использование в ИСПДн беспроводных соединений (в частности 802.11xWi-Fi, 802.15.1 Bluetooth, 802.22WRAN, IrDA и иных беспроводных соединений) в соответствии с задачами (функциями) ИСПДн,для решения которых такие соединения необходимы;

− предоставление доступа к параметрам (изменению параметров) настройки беспроводных соединений только Администратору ИСПДн;

− обеспечение возможности реализации беспроводных соединений только через контролируемые интерфейсы (в том числе, путем применения средств защиты информации);

− регистрация и анализ событий, связанных с использованием беспроводных соединений, в том числе для выявления попыток несанкционированного подключения к ИСПДн через беспроводные соединения.

При обеспечении защиты беспроводных соединений в зависимости от их типов реализуются меры по идентификации и аутентификации в соответствии с пунктами 3.1.1, 3.1.2 и 3.1.6 настоящего Положения (ИАФ.1, ИАФ.2, ИАФ.6).

При невозможности исключения установления беспроводных соединений из-за пределов контролируемой зоны должны приниматься меры защищенного удаленного доступа в соответствии с пунктами 3.2.9 и 3.13.1 настоящего Положения (УПД.13,ЗИС.3).

3.14 Подсистема выявления инцидентов и реагирование на них (ИНЦ)

Подсистема выявления инцидентов и реагирования на них обеспечивает обнаружение, идентификацию, анализ инцидентов в ИСПДн, а также принятие мер по устранению и предупреждению инцидентов.

3.14.1 Определение лиц, ответственных за выявление инцидентов и реагирование на них (ИНЦ.1)

Информация о компьютерных инцидентах поступает из следующих источников:

− от Пользователей ИСПДн;

− от лиц, обеспечивающих функционирование (сопровождение, обслуживание,ремонт), обеспечивающих управление (администрирование) ИСПДн и СЗПДн ООО «Клиника Доктор КИТ»,

− из электронных журналов событий информационной безопасности программно-технических средств защиты информации СЗПДн ООО «Клиника Доктор КИТ»

− из информации, полученной в рамках проводимых регулярных мероприятий по мониторингу и контролю обработки ПДн Ответственным за обеспечение безопасности ПДн;

− других механизмов контроля.

Лицом, ответственным за выявление компьютерных инцидентов и за реагирование на них, является Администратор СЗПДн. Права, обязанности и полномочия Администратор СЗПДн по выявлению компьютерных инцидентов и реагированию на них определены в документе ООО «Клиника Доктор КИТ» Руководство администратора системы защиты персональных данных».

3.14.2 Обнаружение, идентификация и регистрация инцидентов (ИНЦ.2)

Выявление (обнаружение) компьютерных инцидентов происходит:

− непосредственно в процессе работы ИСПДн и СЗПДн;

− в процессе проведения регламентных работ (анализа электронных журналов событий, программно-технических средств, общесистемного программного обеспечения и сетевого оборудования, регулярных мероприятий по мониторингу и контролю обработки ПДн).

Событие безопасности, возникающее в процессе эксплуатации ИСПДн и СЗПДн, считается компьютерным инцидентом, если оно обладает одним или несколькими из следующих признаков:

− нарушение требований законодательства Российской Федерации,нормативных актов ФСБ России и ФСТЭК России, локальных актов ООО «Клиника Доктор КИТ» по обеспечению безопасности ПДн;

− нарушение в выполнении технологических процессов обработки ПДн в ИСПДн;

− несанкционированные и (или) нерегламентированные действия в отношении ИСПДн и СЗПДн;

− хищение (или попытка хищения) информации и (или) осуществление несанкционированного доступа и управления ИСПДн и СЗПДн;

− нанесение ущерба ООО «Клиника Доктор КИТ» и субъектам ПДн.

Перечень наиболее распространенных компьютерных инцидентов:

− сбой в работе программного обеспечения ИСПДн («зависание» компьютера, ошибки в работе программы и т.п.);

− отключение электричества в результате компьютерной атаки;

− обнаружение вредоносного программного обеспечения;

− обнаружение утечки информации (взлом учетной записи пользователя, обнаружение посторонних устройств в системном блоке и т.п.);

− попытка несанкционированного доступа (обнаружены попытки подбора пароля, доступ постороннего лица в помещение и т.п.);

− взлом ИСПДн или СЗПДн или несанкционированный доступ в ИСПДн или

СЗПДн;

− потеря данных (отсутствие возможности сохранить внесенные данные ,отсутствие связи с сервером, повреждение файлов и т.п.);

− выход из строя сервера в результате компьютерной атаки;

- сбой в локальной вычислительной сети (отсутствие доступа в локальной вычислительной сети , отсутствие связи с сервером и т.п.);

− физическое повреждение локальной вычислительной сети или средств вычислительной техники (не включается персональный компьютер, при попытке включения отображается синий или черный экраны, повреждены провода и т.п.).

Администратор СЗПДн регистрирует компьютерные инциденты путем внесения сведений о них в Журнал событий и компьютерных инцидентов (далее - Журнал).

Форма Журнал событий и компьютерных инцидентов, а также порядок регистрации компьютерных инцидентов приведены в документе ООО «Клиника Доктор КИТ»

. Руководство администратора системы защиты персональных данных». Срок хранения Журнала –

не менее 5 лет со дня последней записи в нем.

На основании информации, собранной в соответствии с пунктом 3.14.4 настоящего Положения (ИНЦ.4), Администратором СЗПДн оформляется (в электронном виде либо на бумажном носителе) карточка компьютерного инцидента (далее - Карточка). В ходе проведения служебного расследования компьютерного инцидента в Карточку, при необходимости, вносятся новые или уточненные данные по возникшему компьютерному инциденту. Форма карточки компьютерного

инцидента, а также порядок ее заполнения приведены в документе ООО «Клиника Доктор КИТ».

Руководство администратора системы защиты персональных данных». Карточки компьютерных инцидентов хранятся не менее 5-ти лет.

Ответственный за обеспечение безопасности ПДн ведет единую электронную базу карточек компьютерных инцидентов. Карточка вносится в единую базу в срок, не превышающий 3-х рабочих дней со дня закрытия компьютерного инцидента. Порядок ведения единой электронной базы карточек компьютерных инцидентов приведен в документе ООО «Клиника Доктор КИТ». Инструкция лица, ответственного за обеспечение безопасности персональных данных».

3.14.3 Своевременное информирование лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в информационной системе пользователями и

администраторами (ИНЦ.3)

При возникновении компьютерного инцидента во время работы Пользователь ИСПДн, обнаруживший компьютерный инцидент, незамедлительно ставит в известность Администратора СЗПДн или Ответственного за обеспечение безопасности ПДн (в случае, если поставить в известность Администратора СЗПДн не представляется возможным).

Администратор СЗПДн проводит предварительный анализ компьютерного инцидента и в рамках своих полномочий осуществляет первичную оценку по критерию отнесения события безопасности к компьютерному инциденту. Если наличие компьютерного инцидента подтвердилось, незамедлительно ставит в известность Ответственного за обеспечение безопасности ПДн.

3.14.4 Анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий (ИНЦ.4)

Каждый зафиксированный компьютерный инцидент анализируется с целью дальнейшего предотвращения подобных компьютерных инцидентов в будущем.

Установление причин компьютерного инцидента проводится в две стадии:

− первичный анализ компьютерного инцидента;

− комплексный анализ компьютерного инцидента.

Задачами первичного анализа компьютерного инцидента являются:

− установление обстоятельств и возможных последствий компьютерного инцидента;

− своевременное установление обстоятельств компьютерного инцидента.

Задачами комплексного анализа компьютерного инцидента являются:

− установление причин компьютерного инцидента;

− установление фактических последствий компьютерного инцидента.

Результаты анализа компьютерных инцидентов фиксируются Администратором СЗПДн в карточке компьютерного инцидента в соответствии с пунктом 3.14.2

настоящего Положения (ИНЦ.2).

3.14.5 Принятие мер по устранению последствий инцидентов (ИНЦ.5)

3.14.5.1 Реагирование на компьютерные инциденты В целях предотвращения дальнейшего распространения и устранения причин возникновения компьютерного инцидента производится его локализация и устранение (ликвидация последствий компьютерного инцидента), а также принимаются меры по восстановлению функционирования и проверке работоспособности ИСПДн и СЗПДн.

Ответственный за обеспечение безопасности ПДн в ходе реагирования на компьютерные инциденты и принятия мер по ликвидации последствий компьютерных инцидентов осуществляет:

− совместно с Администратором СЗПДн анализ компьютерных инцидентов (включая определение очередности реагирования на них) в соответствии с пунктом 3.14.4 настоящего Положения (ИНЦ.4);

− проведение мероприятий по ликвидации последствий компьютерных инцидентов в зависимости от результата анализа компьютерного инцидента в соответствии с пунктом 3.14.4 настоящего Положения (ИНЦ.4);

− восстановление функционирования ИСПДн и СЗПДн. Перед принятием мер по ликвидации последствий компьютерных инцидентов определяется:

− состав подразделений и должностных лиц ООО «Клиника Доктор КИТ» ответственных за проведение мероприятий по реагированию на компьютерные инциденты и принятие мер по ликвидации их последствий, их задачи в рамках принимаемых мер;

− перечень средств, необходимых для принятия мер по ликвидации последствий компьютерных инцидентов;

− перечень мер по восстановлению функционирования ИСПДн и СЗПДн и очередность их выполнения.

В процессе восстановления функционирования ИСПДн и СЗПДн собирается необходимая информация о компьютерном инциденте для выяснения причин его возникновения и проведения служебного расследования по факту компьютерного инцидента.

3.14.5.2 Закрытие компьютерного инцидента

Решение о закрытии (завершении) компьютерного инцидента принимается

после:

− полного восстановления функционирования и проверки работоспособности

ИСПДн и СЗПДн;

− полного устранения последствий реализовавшихся в следствие компьютерного инцидента угроз безопасности ПДн при их обработке в ИСПДн;

− выяснения всех причин возникновения и проявлений компьютерного инцидента.

Информация о закрытии компьютерного инцидента отмечается в карточке компьютерного инцидента в соответствии с пунктом 3.14.2 настоящего Положения (ИНЦ.2).

3.14.5.3 Проведение служебных расследований

По факту возникшего компьютерного инцидента в ООО «Клиника Доктор КИТ» проводится служебное расследование. В ходе служебного расследования анализируется собранная в ходе определения, анализа и устранения последствий компьютерного инцидента информация в виде объяснительных и (или) служебных записок от руководителей структурных подразделений ООО «Клиника Доктор КИТ» подчиненных им работников, в зоне ответственности которых произошел компьютерный инцидент.

При необходимости к служебным расследованиям могут привлекаться внешние эксперты в области информационной безопасности.

По результатам служебного разбирательства оформляется служебная записка руководителю (или иному уполномоченному лицу) или иной внутренний документ (далее – Документ по результатам служебного разбирательства), в котором указываются:

− события (в хронологическом порядке) по возникшему компьютерному

инциденту;

− причины возникновения компьютерного инцидента;

− работники ООО «Клиника Доктор КИТ» по вине которых возник компьютерный инцидент (если таковые имеются);

− причиненный компьютерным инцидентом ущерб ООО «Клиника Доктор КИТ и (или) субъектам ПДн (если таковой имеется).

В Документе по результатам служебного разбирательства также определяются необходимые и (или) рекомендуемые меры по предупреждению повторного возникновения компьютерного инцидента, а также сроки их реализации.

При необходимости к Документу по результатам служебного разбирательства прилагается вся собранная при проведении служебного расследования информация от работников ООО «Клиника Доктор КИТ» служебные записки и (или) объяснительные записки работников ООО «Клиника Доктор КИТ». Ставрополя, в зоне ответственности которых произошел компьютерный инцидент, распечатки журналов событий безопасности ИСПДн и СЗПДн, отчеты специализированных систем по мониторингу событий безопасности (если таковые имеются) и иная информация по компьютерному инциденту.

3.14.6 Планирование и принятие мер по предотвращению повторного возникновения инцидентов (ИНЦ.6)

Ответственный за организацию обработки ПДн совместно с Ответственным за обеспечение безопасности ПДн периодически, не реже 1 (одного) раза в год, проводят анализ зарегистрированных компьютерных инцидентов для выработки мероприятий

по их предотвращению. На основании проведенного анализа принимаются превентивные меры по предотвращению компьютерных инцидентов в ИСПДн и СЗПДн.

Превентивные меры противодействия компьютерным инцидентам включают:

− планирование мероприятий по обеспечению безопасности ПДн при их обработке в ИСПДн на случай возникновения компьютерных инцидентов;

− обучение и отработка действий персонала по обеспечению безопасности ПДн при их обработке в ИСПДн в случае возникновения компьютерных инцидентов;

− создание альтернативных мест хранения и обработки ПДн на случай возникновения компьютерного инцидента;

− резервирование программных и программно-аппаратных средств, в том числе средств защиты информации, каналов связи на случай возникновения компьютерного инцидента;

− обеспечение возможности восстановления ПДн, а также восстановления ИСПДн и СЗПДн и (или) их компонентов в случае возникновения компьютерного инцидента;

− определение порядка анализа возникших компьютерных инцидентов и принятия мер по недопущению их повторного возникновения.

В общем случае для предотвращения и минимизации последствий компьютерных инцидентов необходимо четкое соблюдение требований локальных актов ООО «Клиника Доктор КИТ» и инструкций по эксплуатации оборудования, программного обеспечения и средств защиты информации.

3.15 Подсистема управления конфигурацией информационной системы и системы защиты персональных данных (УКФ)

Подсистема управления конфигурацией ИСПДн и СЗПД обеспечивает управление изменениями конфигурации информационной системы и системы защиты ПД н, анализ потенциального воздействия планируемых изменений на обеспечение безопасности ПДн, а также документирование этих изменений.

3.15.1 Определение лиц, которым разрешены действия по внесению изменений в конфигурацию информационной системы и системы защиты персональных данных (УКФ.1)

Определение лиц, которым разрешены действия по внесению изменений в конфигурацию ИСПДн и СЗПДн ООО «Клиника Доктор КИТ» осуществляется на основании соответствующих приказов, утверждаемых руководителем (или иным уполномоченным лицом).

К лицам, которым разрешены действия по внесению изменений в конфигурацию ИСПДн и СЗПДн в частности относятся:

− Администраторы СЗПДн - лица, которым разрешены действия по внесению изменений в конфигурацию СЗПДн и средств защиты информации;

− Администраторы ИСПДн - лица, которым разрешены действия по внесению

изменений в конфигурацию ИСПДн, включающие в том числе:

о системных администраторов средств вычислительной техники ИСПДн;

о администраторов сетевой инфраструктуры;

о администраторов виртуальной инфраструктуры

о администраторов прикладного программного обеспечения ИСПДн;

о и иных лиц, обеспечивающих функционирование (сопровождение,

обслуживание, ремонт) и управление (администрирование) ИСПДн.

Права, обязанности и полномочия указанных лиц определены в следующих документах:

−ООО «Клиника Доктор КИТ» Руководство администратора системы защиты персональных данных»;

− ООО «Клиника Доктор КИТ» Инструкция администратора информационной системы персональных данных».

3.15.2 Управление изменениями конфигурации информационной системы и системы защиты персональных данных (УКФ.2)

Управление изменениями конфигурации ИСПДн и СЗПДн ООО «Клиника Доктор КИТ» (далее управление конфигурацией) осуществляют Администраторы СЗПДн и Администраторы ИСПДн в соответствии с их ролями, определенными в пункте 3.15.1 настоящего Положения (УКФ.1).

Управление конфигурацией ИСПДн и СЗПДн включает:

− определение перечня программных и программно-аппаратных средств ИСПДн и СЗПДн, изменения которых подлежат контролю (определение перечня компонентов программного обеспечения ИСПДн и СЗПДн, подлежащих установке и контроль за установкой компонентов программного обеспечения ИСПДн и СЗПДн осуществляется в соответствии с пунктом 3.3.1настоящего Положения (ОПС.2));

− формирование эталонных версий программного обеспечения и эталонных конфигураций программных и программно-аппаратных средств ИСПДн и СЗПДн;

− организация согласованных процессов изменения конфигурации программных и программно-аппаратных средств ИСПДн и СЗПДн лицами,

указанными в пункте 3.15.1 настоящего Положения (УКФ.1), в части их касающейся (в том числе согласование с Ответственным за обеспечение безопасности ПДн в соответствии с пунктом 3.15.3 настоящего Положения (УКФ.3));

− анализ потенциального воздействия планируемых изменений в конфигурации программных и программно-аппаратных средств ИСПДн и СЗПДн на обеспечение безопасности ПДн в соответствии с пунктами 3.3.1, 3.8.2, 3.15.3 настоящего Положения (ОПС.2, АНЗ.2, УКФ.3);

− учет (документирование) состояний конфигурации и изменений конфигурации программных и программно-аппаратных средств ИСПДн и СЗПДн в соответствии с пунктом 3.15.4 настоящего Положения (УКФ.4).

3.15.3 Анализ потенциального воздействия планируемых изменений в конфигурации информационной системы и системы защиты персональных данных на обеспечение защиты персональных данных и согласование изменений в конфигурации информационной системы с должностным лицом (работником), ответственным за обеспечение безопасности персональных данных (УКФ.3)

Администраторы ИСПДн и СЗПДн осуществляют анализ потенциального воздействия планируемых изменений в конфигурации ИСПДн и СЗПДн на обеспечение безопасности ПДн и согласовывают изменения в конфигурации ИСПДн и СЗПДн с Ответственным за обеспечение безопасности ПДн в соответствии с документами:

− ООО «Клиника Доктор КИТ» Инструкция лица, ответственного за обеспечение безопасности персональных данных»;

−ООО «Клиника Доктор КИТ» Руководство администратора системы защиты персональных данных»;

−ООО «Клиника Доктор КИТ». Инструкция администратора информационной системы персональных данных».

3.15.4 Документирование информации (данных) об изменениях в конфигурации информационной системы и системы защиты персональных данных (УКФ.4)

Администраторы ИСПДн и СЗПДн осуществляют документирование информации (данных) об изменениях в конфигурации ИСПДн и СЗПДн в части их касающейся в соответствии с документами:

−ООО «Клиника Доктор КИТ» Руководство администратора системы защиты персональных данных»;

− ООО «Клиника Доктор КИТ» Инструкция администратора информационной системы персональных данных».

Документированию подлежат:

− изменения эталонных версий программного обеспечения и эталонных конфигураций программных и программно-аппаратных средств ИСПДн и СЗПДн;

− изменения конфигураций программных и программно-аппаратных средств ИСПДн и СЗПДн, вносимые Администраторами ИСПДн и СЗПДн.

Контроль документирования информации (данных) об изменениях в конфигурации ИСПДн и СЗПДн осуществляется Ответственным за обеспечение безопасности ПДн в рамках проводимых регулярных мероприятий по мониторингу и контролю обработки ПДн в соответствии с документом

ООО «Клиника Доктор КИТ» Инструкция лица, ответственного за обеспечение безопасности персональных данных».

4 ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

Изменения и дополнения в настоящее Положение вносятся посредством внесения изменений либо утверждения новой редакции настоящего Положения в установленном в ООО «Клиника Доктор КИТ» порядке.

В случае изменения законодательства Российской Федерации и внутренних документов ООО «Клиника Доктор КИТ» настоящее Положение действует в части, не противоречащей внесенным изменениям.

Изменение наименований структурных подразделений ООО «Клиника Доктор КИТ», перечисленных в настоящем Положении, без существенного изменения фактического функционала структурных подразделений не влечет необходимости актуализации настоящего Положения.

По вопросам, не урегулированным настоящим Положением, работники ООО «Клиника Доктор КИТ» руководствуются действующим законодательством Российской Федерации и внутренними документами. Изменения в настоящее Положение вносятся в следующих случаях:

− по решению руководства на основе периодически проводимых Ответственным за обеспечение безопасности ПДн аудитов безопасности ПДн;

− при изменении законодательных актов Российской Федерации, регулирующих отношения в соответствующей области;

− при изменении нормативных актов регуляторов.

Настоящее Положение вступает в силу со дня его утверждения руководителем и действует до утверждения его новой редакции.