МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
«Тольяттинский государственный университет»

Институт математики, физики и информационных технологий
(наименование института полностью)

Кафедра «Прикладная математика и информатика»
(наименование)

09.04.03 Прикладная информатика
(код и наименование направления подготовки)

Информационные системы и технологии корпоративного управления
(направленность (профиль))

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА (МАГИСТЕРСКАЯ ДИССЕРТАЦИЯ)

на тему «Обеспечение комплексной информационной безопасности в организации»

Студент Н.П. Бабиченко _____
(И.О. Фамилия) (личная подпись)

Научный руководитель канд. пед. наук, доцент Е.В. Панюкова
(ученая степень, звание, И.О. Фамилия)

Тольятти 2020

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Актуальность исследования. Совершенствование информационных технологий и непрерывность процесса информатизации является характерной особенностью развития современного общества. Интеграция IT-технологий во все сферы жизнедеятельности людей привела к необходимости создания информационной инфраструктуры, способной обеспечить сохранность и безопасность конфиденциальных данных. Учитывая повсеместное внедрение передовых технологий в разные отрасли общества, возникают проблемы информационной безопасности (ИБ) организаций, которые с каждым годом становятся все более сложными и разноплановыми [21,33].

Не стала исключением и сфера оказания медицинских услуг. В данной области остро стоит вопрос информационной безопасности. В результате интеграции высокотехнологичного оборудования и информационных систем (ИС) во все области и организации здравоохранения в связи с расширением спектра предоставляемых медицинских услуг, проблема защиты информации приобрела особую актуальность и значимость, вызвав необходимость разработки и внедрения инновационных решений по части обеспечения информационной безопасности медицинских учреждений [25, 34, 31].

Масштабность и неоднородность информационных структур предприятий медицины и здравоохранения приводит к высокой уязвимости информационных систем медицинских учреждений. Менее защищенными оказываются целые структуры, а не отдельно взятые узлы, что связано с повышением сложности инструментов и средств программно-аппаратного обеспечения компаний, а также с определенными недостатками самих информационных технологий [15].

Действующие нормы Федеральных законов и других руководящих документов требуют обеспечения комплексной информационной защиты медицинских учреждений как объектов информатизации, что является актуальной проблемой на сегодняшний день. Главной целью внедрения комплексного подхода в области информационной защищенности учреждений

здравоохранения выступает обеспечение доступности и высокой степени безопасности обрабатываемых данных и защиты информации, используемой в рамках предусмотренных законодательством мер, от несанкционированного вмешательства третьих лиц [16].

Отсутствие эффективной защиты, разработанной на основе комплексного подхода к обеспечению информационной безопасности, ведет к возникновению обширного количества угроз, связанных с хищением или уничтожением персональных данных (ПД) – ключевой информации о сотрудниках и пациентах медицинских организаций, а также нарушает штатный порядок работы учреждения. В некоторых ситуациях сбои в функционировании информационных систем оборачиваются значительными финансовыми потерями, а в отдельных случаях могут стать причиной нанесения вреда жизни и здоровью людей. Например, некорректная работа диагностического оборудования приводит к получению недостоверных результатов анализов, а сбои в медицинской аппаратуре несут опасность для жизни и здоровья пациентов. Исходя из этого можно заключить, что проведение исследований в сфере повышения защиты информационной структуры медицинских организаций необходимы как для обеспечения безопасности ИС субъектов здравоохранения, так и для пациентов, получающих любой вид медицинской помощи, включая консультативную [27, 28].

Степень проработанности темы

В настоящее время активно ведется исследование вопроса защиты информации и изучение защищенности информационной инфраструктуры медицинских учреждений в контексте реализации различного вида атак. Однако вопросу обеспечения комплексной информационной безопасности организаций, осуществляющих медицинскую деятельность, в контексте изучения критических информационных инфраструктур (КИИ) почти не посвящено научных работ ввиду недавнего утверждения в 2018 году федерального закона № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» [3].

Представляется необходимым изучить проблему повышения надежности информационных систем медицинской сферы, найти способы обеспечения безопасного функционирования информационной структуры и свести к минимуму риск внешних и внутренних угроз. С этой целью необходимо внедрить механизм повышения защищенности ИС путем разработки и реализации мероприятий, направленных на обеспечение комплексной информационной защиты учреждений [23].

Исходя из этого, **проблематика исследования** заключается в надобности увеличения уровня защищенности информации в медицинских учреждениях за счет обеспечения комплексной информационной безопасности в условиях непрерывного роста числа угроз, способов их реализации, а также требований федеральных законов и других нормативных документов в отношении обработки данных на субъектах критической информационной инфраструктуры.

Отталкиваясь от актуальности и установленной проблемы можно прийти к выводу о необходимости проведения исследовательских работ в направлении обеспечения комплексной информационной безопасности в организациях, осуществляющих медицинскую деятельность.

Объектом исследования является информационная инфраструктура организации, осуществляющей медицинскую деятельность.

Предметом исследования являются методы совершенствования системы информационной безопасности организации, осуществляющей медицинскую деятельность.

Цель работы заключается в повышении уровня безопасности информационных систем организации посредством совершенствования комплексной системы защиты медицинского учреждения. Для достижения обозначенной цели подразумевается решить последующие задачи:

1. Исследовать теоретические аспекты вопроса обеспечения информационной безопасности критических информационных инфраструктур посредством анализа существующих подходов и принципов.

2. Провести анализ методов обеспечения информационной безопасности критической информационной инфраструктуры.

3. Провести анализ деятельности и исследовать текущий уровень информационной безопасности систем организации, осуществляющей медицинскую деятельность.

4. Провести анализ уязвимостей и угроз информационной безопасности объектов критической информационной инфраструктуры организации, осуществляющей медицинскую деятельность.

5. Разработать модели нарушителя и актуальных угроз безопасности объектов критической информационной инфраструктуры организации, осуществляющей медицинскую деятельность.

6. Категорировать существующие объекты критической информационной инфраструктуры организации, осуществляющей медицинскую деятельность.

7. Усовершенствовать существующую систему защиты организации, осуществляющей медицинскую деятельность, за счет подбора оптимального комплекса мер и использования методов информационной безопасности в части соответствия ФЗ № 187.

В этой работе выдвигается следующая **гипотеза**: внедрение современных подходов и адаптация существующих методов обеспечения комплексной информационной безопасности является необходимым условием для обеспечения достаточной степени защищенности информационной инфраструктуры организации, осуществляющей медицинскую деятельность.

Теоретическую основу исследования составили труды отечественных и зарубежных ученых, монографии, материалы, периодических научных изданий, диссертаций научно-практических конференций по исследуемой проблематике.

В частности, существенную роль при написании работы сыграли труды таких авторов, как Михалевич И.Ф., Фролов Я.О., Сидоренко В.Л., Азаров С.И., Власенко Е.А., Бойченко О. В., Аношкина А. А., посвященные разным

аспектам обеспечения безопасности критически важных объектов информационных инфраструктур [16, 22, 23, 29, 30, 32].

Методологической основой исследования является совокупность методов научного познания, используемых для достижения поставленной цели:

1. Изучение и анализ научной литературы.
2. Системный анализ и моделирование.
3. Методы индукции и дедукции.

Научная новизна работы заключается в том, что исследование вопроса обеспечения комплексной информационной безопасности в организации, осуществляющей медицинскую деятельность, реализуется в контексте обеспечения безопасности критических информационных инфраструктур.

Теоретическая значимость заключается в возможности применения полученных результатов в исследованиях и работах, посвященных различным аспектам обеспечения безопасности объектов критической информационной инфраструктуры.

Практическая значимость исследования состоит в возможности последующего применения полученных результатов работы коммерческими медицинскими компаниями для разработки и внедрения эффективных комплексных мер по защите информации, спроектированных с учетом положений и требований Федеральных законов и прочих нормативно-правовых документов в области обработки данных субъектов информационных инфраструктур с высокой уязвимостью (критических объектов медицинской сферы).

Этапы исследования:

1. Изучение теоретических аспектов вопроса обеспечения безопасности критических информационных инфраструктур.
2. Освещение деятельности организации, осуществляющей медицинскую деятельность.

3. Разработка моделей нарушителя и актуальных угроз безопасности для информационных систем организации, осуществляющей медицинскую деятельность.

4. Выработка рекомендаций по разработке комплексной системы обеспечения информационной безопасности.

На защиту выносятся:

1. Модель актуальных угроз информационной безопасности информационных систем ООО «Семейная поликлиника».

2. Модели нарушителя и актуальных угроз безопасности объектов критической информационной инфраструктуры ООО «Семейная поликлиника».

3. Проект совершенствования комплексной системы информационной безопасности ООО «Семейная поликлиника» за счет подбора оптимального комплекса мер и использования методов информационной безопасности в части соответствия ФЗ № 187.

Объем и структура диссертации - 87 страницы, которые включают текст, 2 схемы, 11 таблиц, 17 изображений. Диссертация состоит из введения, четырех разделов и заключения.

Первый раздел посвящен освещению теоретических аспектов вопроса обеспечения безопасности критических информационных инфраструктур. Второй раздел посвящен освещению деятельности организации, осуществляющей медицинскую деятельность, с конкретизацией помещений и обрабатываемых данных в этих помещениях и информационных системах организации.

В третьем разделе содержится информация о разработке моделей нарушителя и актуальных угроз безопасности для информационных систем организации, осуществляющей медицинскую деятельность, а также об определение категории выявленных объектов критической информационной инфраструктуры.

Четвертый раздел содержит рекомендации по разработке комплексной системы обеспечения информационной безопасности в целях повышения уровня информационной защиты объектов информационной инфраструктуры организации, осуществляющей медицинскую деятельность.

1. ТЕОРЕТИЧЕСКИЕ АСПЕКТЫ ВОПРОСА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

1.1 Правовые основы понятия критической информационной инфраструктуры

Основной задачей по защите национальных интересов в информационной сфере является обеспечение стабильного и бесперебойного функционирования информационной инфраструктуры. В процессе достижения ключевой цели необходимо подготовить правовую базу для налаживания взаимовыгодного сотрудничества между компаниями, владеющими и управляющими критическими объектами, и органами госбезопасности [27].

26.07.2017 г. был принят ФЗ № 187 «О безопасности критической информационной инфраструктуры Российской Федерации», необходимость принятия которого обусловлена увеличением числа компьютерных атак в мире. Данным законопроектом предусматривается разработка эффективного механизма взаимодействия всех сторон, заинтересованных в обеспечении безопасности критически важной информационной инфраструктуры. [3].

Ключевой задачей принятия Федерального закона стало – создать глобальную государственную систему обнаружения, предупреждения, а также ликвидация последствий компьютерных атак на информационные ресурсы нашей страны, получившей название ГосСОПКА. В результате принятия закона перед главными государственными органами, учреждениями и юридическими лицами возникла необходимость совершенствования информационных систем с учетом новых требований безопасности. В положениях федерального документа закреплены базовые принципы обеспечения защиты критически важной информационной инфраструктуры, прописаны полномочия Президента, Правительства РФ и госорганов, имеющих непосредственное отношение к проектированию, разработке, интеграции и обеспечению безопасности информационных потоков, средств и способов передачи информации. Статьями Федерального Закона № 187 определен перечень прав и обязанностей объектов

критически важной информационной инфраструктуры, порядок их классификации и занесения в реестры [3].

В рамках исследования вопроса обеспечения информационной безопасности критической информационной инфраструктуры в первую очередь необходимо определить фундаментальные понятия и основу ФЗ № 187. Так, автоматизированная система управления определяется как система объединения программного и аппаратного обеспечения, предназначенного для контроля производственного оборудования (механизмы приведения в действие) и процессов, а также управления таким оборудованием и процессами [3].

Безопасность критической информационной инфраструктуры определена как безопасность в условиях стабильного функционирования при реализации компьютерных атак, а значимый объект критической информационной инфраструктуры как объект одной из категорий значимости и который включен в регистр значимых объектов критической информационной инфраструктуры.

Что касается компьютерных атак на критическую информационную инфраструктуру, в ФЗ № 187 атаки определены как целенаправленное воздействие на программное и аппаратное обеспечение объектов критической информационной инфраструктуры и сетях телекоммуникации, используемых для организации взаимодействия таких объектов. При этом компьютерный инцидент определен как факт нарушения и (или) завершение функционирования объекта критической информационной инфраструктуры или телекоммуникационной сети [3].

Непосредственно критическая информационная инфраструктура определена как совокупность объектов критической информационной инфраструктуры, а также сети телекоммуникации, которые используются для организации взаимодействия таких объектов.

Субъектами критической информационной инфраструктуры выступают российские государственные органы, учреждения, юридические лица и индивидуальные предприниматели, деятельность которых непосредственно связана с обеспечением информационной безопасности, а объектами защиты

являются информационные системы, сети телекоммуникаций и автоматизированные системы управления.

На рисунке 1.1 приведена классификация субъектов и объектов информационной инфраструктуры.

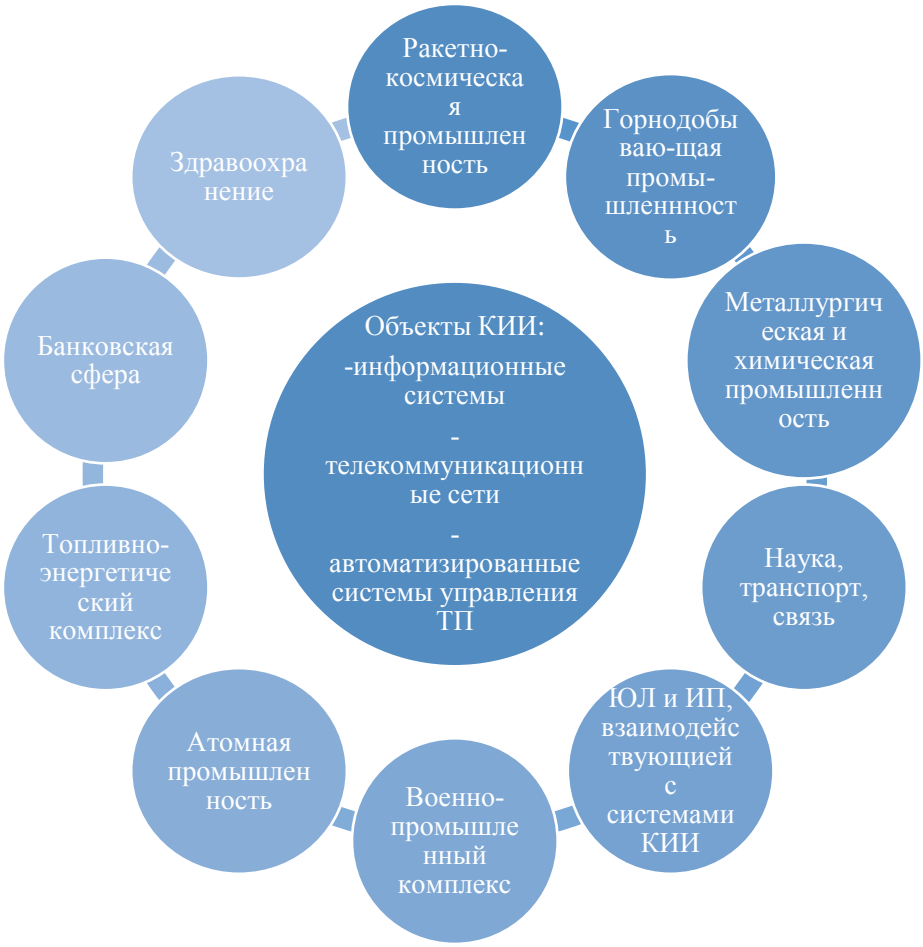

Рисунок 1.1 – Классификация объектов и субъектов критической информационной инфраструктуры

В рамках принятого закона ФЗ № 187 наибольший интерес представляют юридические лица Российской Федерации, осуществляющие деятельность в сфере медицины и здравоохранения, топлива и энергетики, финансов и банковского дела, транспорта и связи, научных исследований, ядерной, горной, химической и металлургической промышленности.

Необходимо отметить, что Федеральным законом № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» обусловлена необходимость субъектов критической информационной

инфраструктуры обеспечения внедрения мер и технических условий для установки и эксплуатации средств, предназначенных для поиска признаков компьютерных атак на уровне подконтрольных им объектов критической информационной инфраструктуры.

В связи с тем, что основной целью является обеспечение безопасности взаимодействия информационных систем и телекоммуникационных сетей, указанных выше субъектов, ключевое место в законе занимают принципы обеспечения безопасности критически важной информационной инфраструктуры, а также порядок организации и проведения проверок безопасности значимых объектов критической информационной инфраструктуры Российской Федерации. В дальнейшей рассмотрим критическую информационную инфраструктуру с позиции порядка и принципов обеспечения безопасности.

1.2 Критическая информационная инфраструктура как объект обеспечения безопасности

В рамках исследования вопроса обеспечения безопасности критической информационной инфраструктуры ФЗ № 187 устанавливает ключевые основы и принципы обеспечения безопасности критически важной информационной инфраструктуры России, в том числе основы функционирования государственной системы обнаружения, предотвращения и ликвидации последствий кибератак в отношении информационных ресурсов Российской Федерации. По сути, это единая система, распределенная по всей стране и наделенная возможностями и ресурсами, необходимыми для обнаружения, предотвращения и ликвидации последствий кибератак и реагирования на кибер-инциденты [3].

Вместе с тем в законе установлены механизмы предотвращения кибер-инцидентов в важных компонентах критической информационной инфраструктуры, что значительно снизит негативное воздействие на страну в случае кибератаки против России, а также определены полномочия

государственных органов по обеспечению безопасности критически важной информационной инфраструктуры, права и обязанности различных субъектов в этой области.

Основной принцип обеспечения безопасности критических информационных инфраструктур заключается в том, что владельцы объектов обязаны обеспечивать их безопасность, в то время как государство оказывает им всяческое содействие. Так, государство должно предоставлять информацию о любых неотложных угрозах информационной безопасности и помогать в проектировании и разработке необходимой программно-аппаратной защиты. В свою очередь, владельцы объектов обязаны информировать органы власти о значительных проблемах, возникших в процессе эксплуатации информационной инфраструктуры [8, 10].

Среди прочего владельцы критических информационных средств инфраструктуры должны:

1. Немедленно сообщить уполномоченным органам о компьютерных инцидентах.

2. Помочь уполномоченным чиновникам в обнаружении, предотвращении и устранении последствий компьютерных атак.

3. Гарантировать сохранность и бесперебойную работу устройств, разработанных с целью обнаружения, предотвращения и устранения компьютерных атак [10].

Закон предусматривает принятие мер, меры нацелены защиту критической информационной инфраструктуры страны от компьютерных атак. Данные меры по обеспечению безопасности критически важной информационной инфраструктуры нашей страны а также информации о состоянии ее безопасности составляют на данный момент составляют государственную тайну.

Общие меры по обеспечению безопасности критической информационной осуществляют органы государственной власти, помимо общих мер функционируют специальная государственная система

обнаружения, а также предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы (ГосСОПКА). В первую очередь рассмотрим правовой статус субъектов государственной власти.

Президент Российской Федерации определяет основные направления государственной политики. За обеспечение безопасности критической информационной инфраструктуры, несут ответственность органы специальной компетенции.

Правительство Российской Федерации определяет механизм категорирования объектов критической информационной инфраструктуры, порядок подготовки и пользования ресурсов сети электросвязи государства для обеспечения функционирования значимых объектов, а также особенности осуществления контроля в данной сфере.

В целях повышения наглядности процесса категорирования объектов критической информационной инфраструктуры Российской Федерации представим рисунок 1 Приложения А, на котором схематично изображена последовательность действий субъектов по выявлению категорий подвластных им объектов.

В роли федерального органа исполнительной власти, ответственного за обеспечение безопасности критической информационной инфраструктуры, была назначена Федеральная служба по техническому и экспортному контролю (ФСТЭК) [4].

В отношении безопасности критической информационной инфраструктуры полномочия ФСТЭК представлены на рисунке 1.2 [5, 7, 12, 13].

В качестве федерального органа исполнительной власти, уполномоченного в области обеспечения функционирования ГосСОПКА на информационные ресурсы РФ, назначена Федеральная служба безопасности.

Программа ГосСОПКА функционирует наряду с органами государственной власти, которые осуществляют общие меры по обеспечению безопасности критической информационной инфраструктуры.

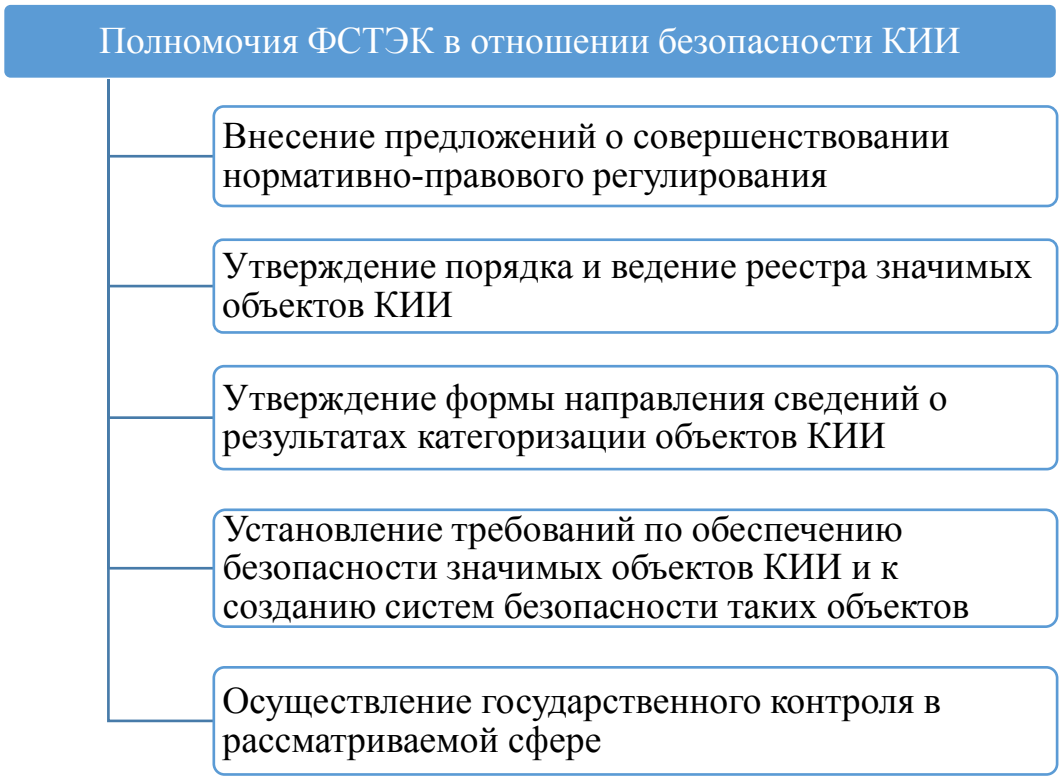

Рисунок 1.2 – Полномочия ФСТЭК в отношении безопасности критической информационной инфраструктуры

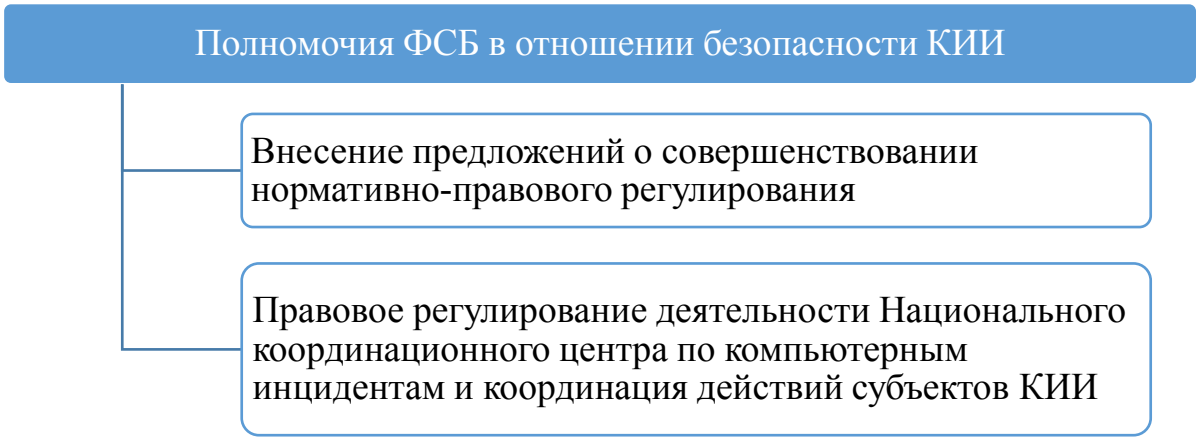

Рисунок 1.3 – Полномочия ФСБ в отношении безопасности критической информационной инфраструктуры

Система была внедрена на объектах после вступления в силу ФЗ № 187 01.01.2018 г., и играет особую роль в механизме обеспечения безопасности информационных ресурсов страны, одновременно являясь превентивной мерой

против компьютерных атак и эффективным способом реагирования на внутренние и внешние угрозы.

На рисунке 1.4 представлены ключевые составляющие системы.

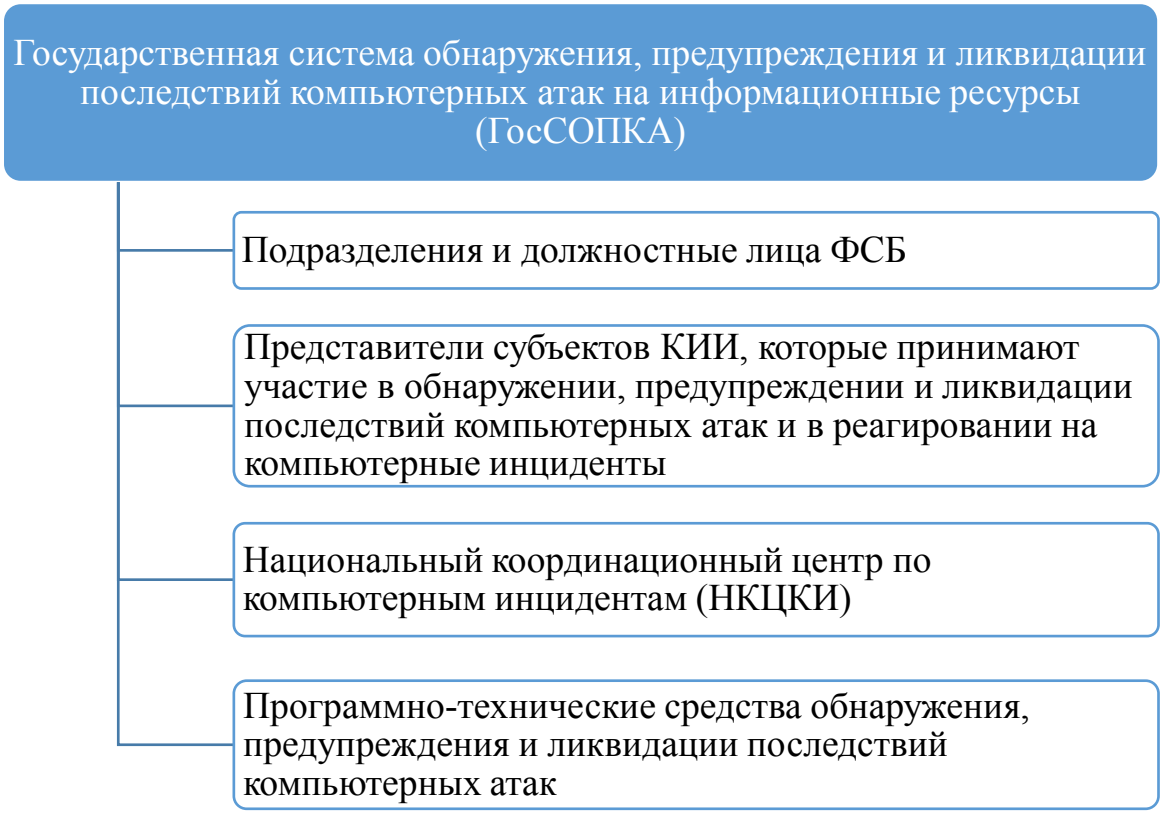

Рисунок 1.4 – Структура государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы

Первостепенная задача НКЦКИ — организация работы субъектов критической информационной инфраструктуры. В связи с этим НКЦКИ (Национальный координационном центре по компьютерным инцидентам) собирает, аккумулирует, систематизирует и оценивает сведения, поступающие от субъектов и ФСТЭК (Федеральная служба по техническому и экспортному контролю). Кроме этого, он организует и реализует обмен этими сведениями.

В целях обеспечения безопасности критической информационной инфраструктуры субъекты должны обеспечить выполнение и реализацию следующих мероприятий, представленных на рисунке 1.5.

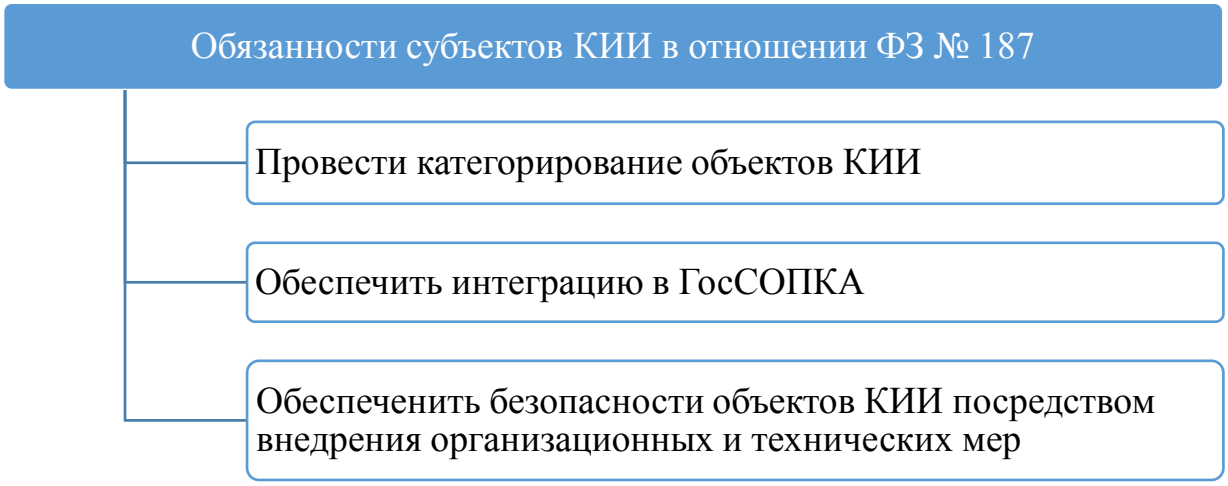

Рисунок 1.5 – Обязанности субъектов критической информационной инфраструктуры в отношении ФЗ № 187

В первую очередь необходимо провести категорирование всех своих объектов критической информационной инфраструктуры и сообщить о них в письменной форме в ФСТЭК для внесения сведений в реестр значимых объектов.

Интеграцией с ГосСОПКА требует от субъекта критической информационной инфраструктуры информирования о компьютерных инцидентах и оказания содействия ФСБ России в обнаружении, предупреждении, а также ликвидации последствий компьютерных атак, помимо этого установить причины и условия возникновения компьютерных инцидентов.

Вместе с тем, на территории объекта критической информационной инфраструктуры может быть размещено оборудование ГосСОПКА.

В этом случае субъект дополнительно обеспечивает его сохранность и бесперебойную работу.

Для значимых объектов критической информационной инфраструктуры помимо интеграции в ГосСОПКА субъекты должны обеспечить выполнение и реализацию следующих мероприятий, представленных на рисунке 1.6.

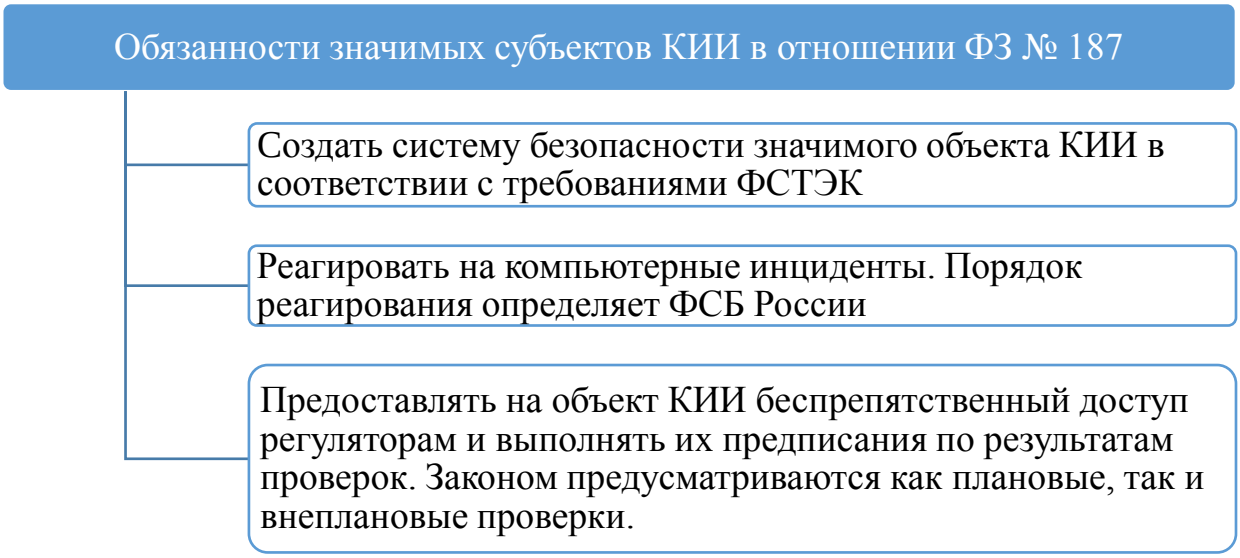

Рисунок 1.6 – Обязанности значимых субъектов критической информационной инфраструктуры в отношении ФЗ № 187

Таким образом, в рамках ФЗ № 187 государство принимает активное и непосредственное участие в безопасности критической информационной инфраструктуры, однако от субъектов требуется соблюдение всех требований и исполнение организационных и технических мероприятий.

1.3 Анализ существующих методов обеспечения информационной безопасности критической информационной инфраструктуры

Способы и инструменты обеспечения информационной безопасности критической информационной инфраструктуры, представляют собой набор программно — аппаратных средств, этических и юридических норм, направленных на противодействие злоумышленникам и минимизации потенциального ущерба собственников информационного комплекса и пользователей информации.

Представим на рисунке 1.7 классификацию методов обеспечения информационной безопасности критической информационной инфраструктуры в контексте организации подхода к обеспечению безопасности.

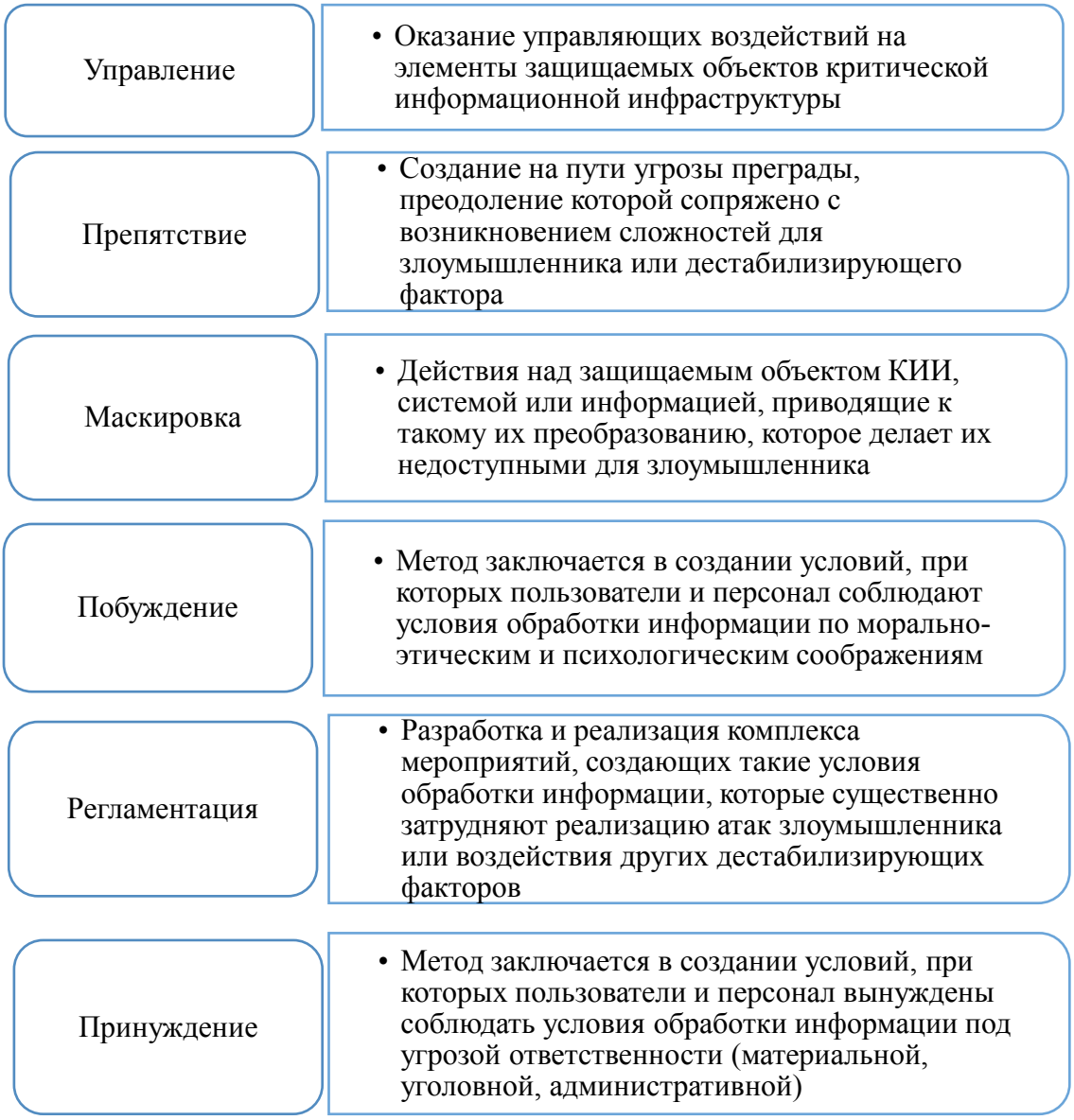

Рисунок 1.7 – Методы обеспечения информационной безопасности критической информационной инфраструктуры

В рамках данной работы ключевой интерес приставляют организационные, программно-аппаратные (технические) и физические методы обеспечения информационной безопасности критической информационной инфраструктуры.

Так, к организационным методам обеспечения информационной безопасности критической информационной инфраструктуры относятся:

1. Организация работы с персоналом.
2. Организация внутри объектового и пропускного режима и охраны.
3. Организация работы с носителями сведений.
4. Комплексное планирование мероприятий по защите информации.
5. Организация аналитической работы и контроля [29].

Правовые методы обеспечения информационной безопасности критической информационной инфраструктуры включают:

1. Патентную защиту.
2. Закон о производственных секретах.
3. Лицензионные соглашения и контракты.
4. Закон об авторском праве [21].

Организационно-правовое обеспечение является многоаспектным понятием, включающим законы, решения, нормативы и правила. Организационно-правовые методы обеспечения информационной безопасности критической информационной инфраструктуры включает:

1. Определение подразделений и лиц, ответственных за организацию обеспечения информационной безопасности критической информационной инфраструктуры.

2. Нормативно-правовые, руководящие и методические материалы (документы) по обеспечению информационной безопасности критической информационной инфраструктуры.

3. Меры ответственности за нарушение правил защиты.

4. Порядок разрешения спорных и конфликтных ситуаций по вопросам обеспечения информационной безопасности критической информационной инфраструктуры [19].

Под технико — математической стороной организационных и правовых методов организации информационной безопасности подразумевается комплекс технических средств, математических способов, прототипов и программных приложений, при содействии которых соблюдаются все

положения и правила, требуемые для правового разделения прав и ответственности в отношении порядка обращения с охраняемой информацией.

Ключевыми из этих положений считают следующие:

1. Закрепление на документе индивидуальных идентификаторов (подписей) лиц, которые изготовили документ и (либо) несущих ответственность за него.

2. Закрепление (при необходимости) на документе индивидуальных идентификаторов (подписей) лиц, ознакомившихся с содержанием.

3. Возможность неприметного (без оставления следов) изменения содержания инфы даже лицами, которые имеют разрешение на доступ к ней, то есть закрепление фактов хоть какого (как разрешенного, так и несогласованного) изменения информации.

4. Закрепление факта хоть какого (как несогласованного, так и разрешенного) копирования защищаемой информации [19].

Под правовыми аспектами организационно-законодательных способов обеспечения информационной безопасности критической информационной инфраструктуры объектов понимается совокупность законов и остальных законов, при помощи которых достигаются последующие цели:

1. Неукоснительное обязанность соблюдение всеми лицами всех правил защиты информации.

2. За несоблюдение норм защиты узакониваются меры ответственности.

3. Технико-математические решения вопросов организационно-законодательного обеспечения защиты информации также узакониваются (приобретают юридическую силу [21].

4. Процессуальные процедуры разрешения ситуаций, которые складываются в процессе деятельности системы защиты также узакониваются.

Способы организации информационной безопасности на физическом уровне — это набор определенных подходов с применением различных устройств различных приспособлений, а также приборов, которые создают препятствия по ходу движения злоумышленников [24].

Физические средства содержит в себе: механические, электрические, радиотехнические приборы для ограничения либо воспрещения несогласованного доступа (НСД), перемещения средств, материалов и остальных возможных видов противоправных действий.

Методы разграничения доступа и физической защиты принято использовать для организации:

1. Охраны территории и наблюдения на которой размещены объекты критической информационной инфраструктуры.
2. Охраны и контроля зданий и внутренних помещений.
3. Охраны информации, оборудования.
4. Контролируемый доступ в здания и внутренние помещения [24].

Можно разделить физические средства обеспечения информационной безопасности критической информационной инфраструктуры на три категории:

1. Средства предупреждения.
2. Средства обнаружения.
3. Системы ликвидации угроз.

В общем случае все средства физической защиты объектов критической информационной инфраструктуры можно разделить на следующие группы:

1. Охранные и охранно-пожарные системы.
2. Охранное телевидение.
3. Охранное освещение.
4. Средства физической защиты.

К средствам физической защиты относятся:

1. Ограждение и физическая изоляция.
2. Запирающие устройства.
3. Системы разграничения доступа.

К системам разграничения доступа относятся:

1. Системы, использующие различные карты и карточки, на которых помещается кодированная или открытая информация о владельце.
2. Системы опознавания по отпечаткам пальцев.

3. Системы опознавания по голосу.
4. Системы опознавания по почерку.
5. Система опознавания по геометрии рук.

Необходимо также отметить, что в соответствие с Приказом ФСТЭК от 25.12.2017 №239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» для значимых объектах критической инфраструктуры в зависимости от категории значимости и выявленных угроз безопасности информации должны быть определены и внедрены организационные меры и технические средства обеспечения безопасности [11].

Таким образом, в дальнейшей работе необходимо провести подробный анализ актуальных угроз информационной безопасности применительно к объекту исследования, на основании проведенного анализа можно сделать вывод о том, что для обеспечения безопасности критической информационной инфраструктуры должны быть четко определены требования и принципы информационной безопасности с целью повышения эффективности методов защиты информации и построения эффективной комплексной системы информационной безопасности в организации.

1.4 Принципы обеспечения комплексной безопасности критической информационной инфраструктуры

Сегодня безопасность уже не ограничивается установкой отдельного устройства, и должна быть обеспечена на уровне каждого пакета, сервиса или компонента объекта критической информационной инфраструктуры. Средства защиты информации (СрЗИ) должны быть распределены по всей рабочей среде объекта критической информационной инфраструктуры и поддерживать следующие условия:

1. Доступность и надежность сервисов.
2. Непрерывность деловой активности.
3. Заданный уровень обслуживания и эффективности работы системы.

Создание надежно защищенных объектов критической информационной инфраструктуры представляет из себя всеохватывающую дилемму, которая включает:

1. Обеспечение конфиденциальности информации, которая хранится, обрабатывается и передается по каналам связи.

2. Обеспечение контроля доступа к информационным ресурсам объектов критической информационной инфраструктуры в соответствии с полномочиями пользователей, а также целостность и идентификация хранимой и передаваемой информации.

3. Предотвращение утечки информации, циркулирующей в объектах критической информационной инфраструктуры.

4. Исключение несанкционированного доступа к информации при ее хранении и обработке в объектах критической информационной инфраструктуры, а также предотвращение программных воздействий либо их последствий, вызывающих искажение информации либо ее уничтожение.

5. Реализацию необходимых организационно-технических мер по обеспечению информационной безопасности объектов критической информационной инфраструктуры [11].

В целях организации безопасности разрабатываются и внедряются комплексные системы обеспечения безопасности, которые представляют собой совокупность организационных и инженерно-технических мероприятий, которые направлены на обеспечение защиты информации от разглашения, утечки и несанкционированного доступа. Основные требования к комплексной системе обеспечения безопасности критической информационной инфраструктуры можно перечислить в следующем перечне:

1. Разработка на основе положений и требований существующих законов, стандартов и нормативно-методических документов по обеспечению информационной безопасности.

2. Использование комплекса программно-технических средств и организационных мер для защиты системы.

3. Надежность, производительность, конфигурируемость.

4. Экономическая целесообразность.

5. Выполнение на всех этапах жизненного цикла обработки информации.

6. Возможность совершенствования.

7. Обеспечение разграничения доступа к конфиденциальной ин-формации с отвлечением нарушителя на ложную информацию (обеспечение не только пассивной, но и активной защиты).

8. Взаимодействие с незащищенными системами по установленным для этого правилам разграничения доступа.

9. Обеспечение проведения учета и расследования случаев нарушения безопасности информации.

10. Возможность оценки эффективности ее применения.

Для объединения инструментов организации безопасности потребуется основополагающий прототип работы и устойчивая инфраструктура, лежащая в основе организации постоянной активности.

Требуется, что бы все сегменты сетевой иерархии объектов проблемной информационной структуры владели сведениями о существенных моментах работы системы в общем, а сам объект проблемной информационной структуры стал динамичной областью отслеживания и осуществления стратегии безопасности [11].

Другими словами, безопасность становится критически важной характеристикой работы субъектов критической информационной инфраструктуры и играет важнейшую роль. Обеспечение комплексной безопасности должно быть реализовано в первую очередь посредством перехода от традиционного реактивного подхода к поэтапному проактивному подходу, уменьшая количество существующих уязвимостей, улучшая показатели времени реакции и эффективность подавления атак [11].

Таким образом, принципы обеспечения комплексной безопасности критической информационной инфраструктуры можно определить в следующем перечне:

1. Законность.
2. Непрерывность участия на должном уровне уполномоченных федеральных органов исполнительной власти.
3. Приоритет в пользу предотвращения компьютерных атак.
4. Системность (разработка алгоритмов, учитывая также и внешние факторы).
5. Комплексность.
6. Непрерывность защиты.
7. Разумная достаточность (экономическая эффективность).
8. Гибкость управления и применения.
9. Открытость алгоритмов и механизмов защиты.
10. Простота применения защитных мер и средств.
11. Превентивность.

В пределах приведенного исследования по организации системной информационной безопасности проблемных информационных структур надо брать в расчет основные правила устранения угроз информационной безопасности:

1. Предотвращение. Осуществление защитных мер по предупреждению известных опасностей. Ликвидация опасностей подразумевает использование ряда инструментов, включающих как типовые, так и улучшенные варианты программного обеспечения, специализированных межсетевых экранов или иных аналогов для разграниченного доступа в систему.

2. Мониторинг. Чтобы определять реальные или потенциальные рискованные поведенческие действия пользователей необходимо осуществлять процедуру мониторинга. Она позволяет, особенно в уязвимых областях, предугадывать опасности.

3. Важно разделять причины возникновения угроз и конфликтов в информационной системе. Они могут носить либо целенаправленный характер (преднамеренные действия злоумышленников), либо являться результатом ошибок. В первом случае следует выявлять источник угрозы и его блокировать, во втором – минимизировать случайные изменения данных системы из-за невнимательности, неосведомленности или халатности пользователей. Необходимо фиксировать и отслеживать атаки, анализировать логи журналов и сетевых экранов (брандмауэров).

4. Ответные меры.

Если обнаружена попытка несанкционированного вмешательства в информационную систему, требуется оперативное (чаще – в режиме реального времени) вмешательство. Все шаги должны быть проработаны заранее, чтобы не терять время, которое потом способно вылиться в существенные убытки [6].

1.5 Выводы по разделу 1

Исходя из проведенного исследования вопроса обеспечения комплексной информационной безопасности критической информационной инфраструктуры можно сделать вывод об актуальности изучаемого вопроса.

Таким образом, в дальнейшей работе необходимо:

1. Провести анализ деятельности и исследовать текущий уровень информационной безопасности систем организации, осуществляющей медицинскую деятельность.

2. Провести анализ уязвимостей и угроз информационной безопасности объектов критической информационной инфраструктуры организации, осуществляющей медицинскую деятельность.

3. Разработать модели нарушителя и актуальных угроз безопасности объектов критической информационной инфраструктуры организации, осуществляющей медицинскую деятельность.

4. Категорировать существующие объекты критической информационной инфраструктуры организации, осуществляющей медицинскую деятельность.

5. Усовершенствовать существующую систему защиты организации, осуществляющей медицинскую деятельность, за счет подбора оптимального комплекса мер и использования методов информационной безопасности в части соответствия ФЗ № 187.

В работе были проанализированы ключевые аспекты ФЗ № 187 и определены принципы обеспечения комплексной безопасности объектов критической информационной инфраструктуры, на основании чего можно сделать вывод о необходимости повышения уровня информационной безопасности объектов критических информационных инфраструктур посредством совершенствования комплексной системы защиты.

2 ИССЛЕДОВАНИЕ ВОПРОСА НЕОБХОДИМОСТИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ, ОСУЩЕСТВЛЯЮЩЕЙ МЕДИЦИНСКУЮ ДЕЯТЕЛЬНОСТЬ

2.1 Изучение деятельности и организационной структуры организации, осуществляющей медицинскую деятельность

В рамках данной работы ключевой интерес представляет деятельность исследуемой организации ООО «Семейная поликлиника», оказывающей широкий спектр медицинских услуг в городе Магадане с 2007 года.

Рабочие места сотрудников поликлиники размещены на территории организации по адресу Магадан, ул. Пролетарская, д. 14. Здание, в котором расположена поликлиника, представляет собой 6-этажное строение, на первом этаже которого с отдельным входом расположен административный центр ООО «Семейная поликлиника» и несколько приемных, а на втором кабинеты врачей и оборудование.

ООО «Семейная поликлиника» позволяет пациентам записаться на прием к ряду врачей и специалистов:

1. Терапевт.
2. Аллерголог-иммунолог.
3. Невролог.
4. Оториноларинголог.
5. Эндокринолог.
6. Кардиолог.
7. Гинеколог.
8. Педиатр.
9. Офтальмолог.
10. Уролог.
11. Хирург.
12. Стоматолог.

13. Специалист ультразвуковой и функциональной диагностики.

Исходя из представленной информации о спектре медицинской деятельности ООО «Семейная поликлиника», в первую очередь сформируем обобщенный перечень процессов и услуг поликлиники:

1. Оказание медицинских услуг и медицинской помощи.
   - Амбулаторная медицинская консультативная и лечебная помощь.
   - Восстановительное лечение.
   - Диагностическая медицинская помощь.
   - Высокотехнологическая медицинская помощь.
2. Проведение исследований, клинических испытаний, осмотров.
3. Фармацевтическая деятельность.
4. Деятельность, связанная с использованием источников ионизирующего излучения (рентген, томография, лучевая терапия).
5. Розничная торговля товарами личной гигиены и общего потребления.
6. Проведение конференций, семинаров и иных ученых мероприятий.
7. Управление персоналом.
8. Бухгалтерский учет.
9. Заключение договоров с контрагентами.
10. Обслуживание ИТ-инфраструктуры.
11. Обслуживание инженерных систем.
12. Работа с обращениями клиентов.
13. Претензионная и судебная работа.

Организационная структура ООО «Семейная поликлиника» состоит из ряда подразделений и представлена на рисунке 2.1. По указанному выше адресу на первом этаже расположены финансовый и технический отделы, хозяйственная служба, руководство, административно-управленческий персонал, а также ряд кабинетов врачей.

Рисунок 2.1 – Модель организационной структуры организации ООО «Семейная поликлиника»

На втором этаже размещены кабинеты врачей и процедурные кабинеты, которые для наглядности объединены в подразделения медицинского обслуживания в модели организационной структуры.

2.2 Анализ технической архитектуры организации, осуществляющей медицинскую деятельность

На рисунках 1 и 2 Приложения Б представлены схемы помещений с учетом, в которых располагаются сотрудники организации ООО «Семейная поликлиника».

На данный момент во всех помещениях медицинской организации установлены средства пожарной и охранной сигнализаций. На окнах помещений первого этажа стальные решётки отсутствуют. В рабочее время в помещения служебной части организации обеспечивается пропускной режим при помощи системы контроля и управления доступом (СКУД). В нерабочее

время помещения закрываются на замок и ставятся на сигнализацию, которая выведена на пульт охраны.

Все автоматические рабочие места (АРМ) пользователей объединены в локальную сеть (ЛС) с выходом в Интернет. Топология локальной сети организации ООО «Семейная поликлиника» представлена на рисунках 1 и 2 в Приложении В. Данная топология отображает основные структурные элементы сетевой инфраструктуры поликлиники.

В локальную сеть организации «Семейная поликлиника» входят 29 автоматизированных рабочих мест (АРМ) работников. Для администрирования сети используется следующее серверное оснащение HP ProLiant ML30 Gen9, оно смонтировано в административном подразделении организации.

Для реализации печати и сканирования в локальной сети подключено 18 МФУ Brother DCP-7057WR, подключенных к USB разъему.

Для обеспечения доступа к ресурсам сети существует разделение прав доступа. Каждому работнику присвоено уникальное имя (логин) пароль, необходимые для входа в систему. Кроме этого, для каждого пользователя заведена отдельная папка к которой имеет доступ он и администратор сети. Существует общая папка, необходимая для обмена данными между работниками компании.

В настоящее время в ООО «Семейная поликлиника» используются современные технические средства. Подсистему технического обеспечения исследуемой медицинской организации можно определить следующим перечнем:

1. Технические средства сбора, регистрации, накопления, обработки, отображения, размножения, доставки, сохранения и обеспечения безопасности информации.
2. Компьютеры различных моделей, серверные и сетевые устройства, оргтехника.
3. Телекоммуникационная техника и средства связи.
4. Общесистемная документация, включающая государственные,

отраслевые и корпоративные стандарты по техническому обеспечению.

5. Специализированная документация, содержащая методические материалы по всем этапам проектирования, разработки, внедрения, сопровождения и применения технических и технологических средств.

6. Нормативно–справочная документация для выполнения технического обеспечения.

Технические характеристики аппаратного обеспечения полностью соответствуют потребностям сотрудников и врачей организации ООО «Семейная поликлиника» при решении их трудовых функций и задач. Используемые АРМ имеют различную конфигурацию, но имеют следующие минимальные требования:

1. Процессор с частотой не менее 2.6 ГГц.
2. Оперативная память не менее 3 Гигабайт.
3. Разрешение монитора не менее 1280x1024 пикс.
4. Видеокарта не менее 1024 МБ.
5. Сетевая карта.
6. Операционная система Windows 7 или новее.

Также в аппаратное обеспечение входят источники бесперебойного питания, которые в случае кратковременных сбоев напряжения позволяют работать с системой не менее десяти минут после отключения электричества. Для организации работы сети поликлиники используется один сетевой коммутатор.

2.3 Анализ программной архитектуры и данных, обрабатываемых медицинской организацией

Необходимо учитывать в рамках этой работы, что в данный момент в медицинской организации используются программные продукты. На рисунке 2.2 изображена модель информационной инфраструктуры поликлиники, которая содержит программные продукты MS Office, 1С Предприятия (Зарплата, Кадры, Склад), MS Office, банковское и другое специализированное

программное обеспечение, которое требуется для выполнения основной деятельности поликлиники. В управлении административного отдела поликлиники ООО «Семейная поликлиника» также имеется информационный сайт (https://magdelux.ru/semeynaa_poliklinika), позволяющий клиентам удаленно ознакомиться с деятельностью и услугами медицинской организации.

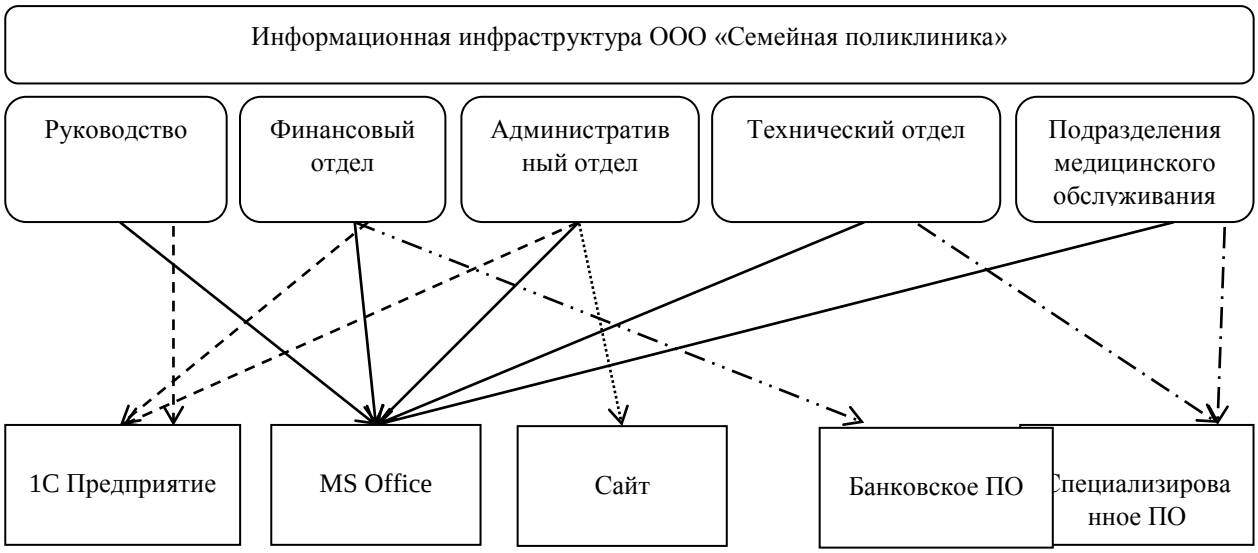

Рисунок 2.2 – Модель информационной инфраструктуры медицинской организации ООО «Семейная поликлиника»

Установленное программного обеспечения на рабочих станциях определенно спецификой деятельности сотрудника, за которым закреплено рабочее место. Несмотря на трудовые функции сотрудника за которым закреплено рабочее место на сервер и рабочую станцию установлено общее программное обеспечение:

1. Стандартный набор программы Microsoft Office: Word, Excel.
2. Антивирус Dr.Web.
3. В качестве браузера используется Mozilla Firefox.

Отдельно стоит отметить, что на сервере организации ООО «Семейная поликлиника» установлена операционная система Windows Server 2012. Эта операционная система используется в современных вычислительных сетях для организации серверов. Данная операционная система обладает отличной функциональностью, высоким быстродействием, а также поддержкой

неограниченного числа подключений.

2.4 Анализ обрабатываемых в медицинской организации данных

В рамках обеспечения комплексной информационной безопасности в организации первым шагом определим какие данные используются в информационных системах поликлиники.

Информационная система компании оперирует персональными сведениями и сведениями, относящимися к врачебной тайне.

Если сведения, относящиеся к врачебной тайне относительно просто выявить, то вопрос выявления и организации защиты личных данных значительно сложнее.

Пункт 1 ст. 3 Федеральных закона от 27 июля 2006 г. N 152-ФЗ «О персональных данных» определяет, что индивидуальные данные — любые сведения так или иначе, относящиеся к любому физическому лицу.

Иными словами, персональные данные представляют собой любую информацию, относящуюся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных).

Данные о пациентах — личные сведения, содержащие данные о событиях и обстоятельствах жизни пациента, допускающие распознание его личности.

К таким сведениям относят биометрию, представляющую параметры субъекта, а именно — группа крови, рост, цвет глаз, вес, анализ дезоксирибонуклеиновой кислоты (ДНК).

Сюда относят и данные, которые возможно извлечь с фото или видеоматериалов с человеком.

Исходя из деятельности ООО «Семейная поликлиника», определим перечень персональных данных пациентов на рисунке 2.3.

Рисунок 2.3 – Перечень персональных данных пациентов медицинской организации ООО «Семейная поликлиника»

Личные данные работников клиники применяют для оформления договорных отношений с нанимателем в границах действия Трудового законодательства.

Эти данные необходимы для заключения трудового контракта и представлены на рисунке 2.4.

Обработка персональных данных пациентов и сотрудников медицинской организации ООО «Семейная поликлиника» осуществляется с использованием информационных систем, в которых операции по обработке персональных данных можно определить следующим перечнем: сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передача (распространение, предоставление, доступ), блокирование, обезличивание, удаление, уничтожение персональных данных.

Анкета, автобиография (заполняется при приеме на работу)	•Анкетные данные сотрудника •биографические данные сотрудника
Копия документа, удостоверяющего личность работника	•Фамилия Имя Отчество •Дата рождения •Адрес регистрации •Семейное положеняи • Состав семьи
Личная карточка (форма N Т-2, утверждена Постановлением Госкомстата России от 05.01.2004 N 1)	•Фамилия Имя Отчество •Место рождения •Состав семьи •Образование •Паспортные данные
Трудовая книжка	•Сведения о трудовом стаже •Сведения о предыдущих местах работы
Копии свидетельств о заключении брака, рождении детей	•Состав семьи •Изменения в семейном положении
Справка с предыдущего места работы	•Фамилия Имя Отчество •Данные о сумме дохода и удержанного НДФЛ
Документы воинского учета	•Информация об отношении работника к воинской обязанности, необходимая работодателю для осуществления воинского учета работников
Документы об образовании	•Подтверждают квалификацию работника, обосновывают занятие определенной должности
Документы обязательного пенсионного страхования	•Фамилия Имя Отчество •Личные данные
Трудовой договор	•Сведения о должности работника, заработной плате, месте работы, рабочем месте, а также иные персональные данные работника
Приказы по личному составу	•Информация о приеме, переводе, увольнении и иных событиях, относящихся к трудовой деятельности работника

Рисунок 2.4 – Перечень персональных данных сотрудников медицинской организации ООО «Семейная поликлиника»

Режим обработки персональных данных в информационных системах поликлиники – многопользовательский. Объём обрабатываемых (одновременно) ПДн – менее чем 100 000 субъектов ПДн, являющихся сотрудниками и клиентами поликлиники. Все компоненты информационных систем обработки персональных данных ООО «Семейная поликлиника» расположены на одном объекте вычислительной техники внутри контролируемой зоны (КЗ) (рисунок 1 и 2 Приложения Б). В работе информационных систем обработки персональных данных поликлиники используются следующие технические средства:

1. Сервер, обрабатывающий персональные данные.
2. Автоматизированные рабочие места (рабочие станции пользователей).
3. Сетевое оборудование, участвующее в передаче персональных данных внутри ИСПДн.
4. Линии ВТСС.
5. Принтеры и многофункциональные устройства (МФУ).
6. Съёмные (отчуждаемые) носители информации.

Исходя из проведенного анализа персональных данных ООО «Семейная поликлиника» всю циркулирующую информацию можно категорировать в соответствие с таблицей 2.1.

Таблица 2.1 - Результаты анализа персональных данных, обрабатываемых в ООО «Семейная поликлиника»

Анализируемый состав персональных данных	Категория персональных данных
Фамилия, имя, отчество (ФИО)	3
Дата рождения	4 (обезличенные)
Паспортные данные	2
Данные о регистрации (включают дату и место регистрации по месту жительства/места жительства)	3
Данные об изменениях должностного положения	4 (обезличенные)
Идентификационный номер налогоплательщика (ИНН), СНИЛС, номер страхового медполиса	3
Финансовые данные	4 (обезличенные)

С учетом требований к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119, выделяются четыре категории персональных данных в рамках информационных систем предприятий, обрабатывающих выявленную в ООО «Семейная поликлиника» информацию [9].

В данном разделе был проведен анализ обрабатываемых данных, который позволил категорировать информацию ООО «Семейная поликлиника».

2.5 Выводы по разделу 2

Таким образом, в данной главе было проведено исследование деятельности и организационной структуры медицинской организации ООО «Семейная поликлиника», включающее изучение общей информация об организации, анализ технической и программной архитектуры, а также существующих информационных систем и данных, обрабатываемых в исследуемой поликлинике.

Первичный анализ показал, что текущий уровень безопасности данных, можно оценить, как неудовлетворительный. Дело в том, что в компании нет минимально необходимых инженерных средств защиты (например, решеток на окнах), четкой документации по порядку получения доступа к персональным данным и врачебной тайне, а также прописанной степени ответственности за разглашение такой информации. Вместе с тем, в помещениях медицинской организации ООО «Семейная поликлиника» отсутствуют система контроля управления доступа, что также является недопустимым в рамках обеспечения доступа разных категорий персонала (административного и управленческого, а также исполнительского уровней).

В дальнейшей работе следует более точно определить текущий уровень информационной безопасности в соответствии с ФЗ № 187 посредством проведения выявления и категорирования объектов критической

информационной инфраструктуры, выявления критических процессов, проведения анализа актуальных угроз и других мероприятий, позволяющих определить конкретные требования к комплексу мер и методов, обеспечивающих комплексную информационную безопасность медицинской организации ООО «Семейная поликлиника».

3. КАТЕГОРИРОВАНИЕ ОБЪЕКТА КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ ОРГАНИЗАЦИИ, ОСУЩЕСТВЛЯЮЩЕЙ МЕДИЦИНСКУЮ ДЕЯТЕЛЬНОСТЬ

3.1 Выявление критических процессов и определение объектов критической информационной инфраструктуры организации, осуществляющей медицинскую деятельность

В рамках данного исследования и проведения категорирования медицинской организации ООО «Семейная поликлиника» в первую очередь необходимо сформировать комиссию. В качестве примера можно привести следующий перечень должностей сотрудников:

1. Главный врач
2. Заместитель главного врача по медицинской деятельности
3. Ответственного за информационную безопасность
4. Ответственного за ГОиЧС.
5. Представители организации, оказывающей услуги обеспечения информационной безопасности.

Создание комиссии рекомендуется документировать в форме приказа о создании комиссии для категорирования объектов критической информационной инфраструктуры.

Обобщенный перечень процессов медицинской организации ООО «Семейная поликлиника» был представлен в п. 2.1. По результатам обсуждения комиссией следует выявить возможные последствия от нарушения или прекращения того или иного процесса медицинского учреждения на основании критериев, утвержденных постановлением правительства №127. В результате сформируем перечень критических процессов медицинской организации ООО «Семейная поликлиника», к которым необходимо уделить наше дальнейшее внимание:

1. Оказание медицинских услуг и медицинской помощи.
2. Проведение исследований, клинических испытаний, осмотров.
3. Фармацевтическая деятельность.

4. Деятельность по обороту наркотических средств и психотропных веществ.

5. Деятельности связанная с использованием источников ионизирующего излучения (рентген, томография, лучевая терапия).

6. Сбор, хранение и реализация донорской крови.

7. Услуги длительного пребывания пациентов / госпитализации / стационар.

8. Обслуживание инженерных систем (пожарная сигнализация, электропитание).

На основании проведенного анализа определим перечень объектов критической информационной инфраструктуры медицинской организации ООО «Семейная поликлиника». В целях определения объектов критической информационной инфраструктуры медицинского учреждения перечислим в следующем списке возможные объекты КИИ в связке с процессами ООО «Семейная поликлиника»:

1. Объект КИИ, обслуживающий управленческие процессы.
2. Объект КИИ, обслуживающий финансово-экономические процессы.
3. Объект КИИ, обслуживающий технологические процессы.
4. Объект КИИ, обслуживающий производственные процессы.
5. Объект КИИ, обслуживающий иные процессы.

Таким образом, на ряду с системами обработки персональных данных, выявленных во втором разделе исследования, в ООО «Семейная поликлиника» функционируют автоматизированные системы управления технологическими процессами и корпоративная сеть. Далее перечислим точный перечень объектов критической информационной инфраструктуры исследуемой медицинской организации ООО «Семейная поликлиника» [7]:

1. ИС:
   - "Электронная очередь".
   - "СОЦ-Лаборатория".
   - "Льготные рецепты".

- "М-Аптека".
- МИС "Самсон".
- "Медкомтех".
- "Экспресс-здоровье".
- "Скрининг новорожденных".
- "Высокозатратные нозологии".
- "Регистр больных сахарным диабетом".
- "Кадровый и бухгалтерский учет".
- СК ИПРА.

2. АСУ:
   - АСУ пожаротушением.
   - АСУ рентген аппаратами.
   - АСУ томографом.
   - АСУ лучевой терапия.
3. ИТС:
   - Корпоративная сеть ККБ №0.

Необходимо отметить, что в данном перечне не содержатся внешние защищенные сети, такие как Защищенная сеть Минздрава РФ, Защищенная сеть Минздрава КК, Защищенная сеть ТФОМС, так как рассматриваемая медицинская организация не является владельцем данных сетей.

На основании данного перечня следует определить список тех объектов, которые обрабатывают выявленные ранее критические процессы, после чего получившийся, предварительный, но ещё не утвержденный, перечень объектов критической информационной инфраструктуры необходимо направить вышестоящему государственному органу (Минздрав субъекта РФ). После согласования перечня с отраслевым регулятором, готовится документ с перечнем объектов и направляется письмо на начальника 2 управления ФСТЭК России (копию на руководителя Управления ФСТЭК России по вашему федеральному округу), в приложении к которому необходимо указать перечень объектов КИИ [7, 12, 13].

3.2 Оценка факторов активности потенциального злоумышленника в контексте информационной безопасности организации, осуществляющей медицинскую деятельность

Реализация угрозы безопасности возможна в результате образования канала реализации между источником угрозы и носителем данных. С точки зрения наличия законного доступа к объектам критической инфраструктуры медицинской организации ООО «Семейная поликлиника» все нарушители делятся на две группы:

1. Внешние нарушители.
2. Внутренние нарушители.

К внешним злоумышленникам относятся физические лица, не имеющие законного доступа к ресурсам объектов критической инфраструктуры медицинского учреждения, и реализующие угрозы при помощи несанкционированного доступа. Для организации таковыми могут являться:

1. Криминальные структуры.
2. Злоумышленники или внешние субъекты.
3. Конкурирующие организации.
4. Недобросовестные разработчики и поставщики.
5. Бывшие сотрудники.

К внутренним злоумышленникам относятся физические лица, имеющие доступ к объектам критической инфраструктуры медицинской организации ООО «Семейная поликлиника», в том числе сами сотрудники медицинских учреждений. К внутренним злоумышленникам в организации могут относиться:

1. Администраторы объектов критической инфраструктуры медицинской организации и администраторы безопасности;

2. Пользователи объектов критической инфраструктуры медицинской организации;

3. Сотрудники, имеющие санкционированный доступ в служебных целях в помещения, в которых размещены ресурсы объектов критической

инфраструктуры медицинской организации, но не имеющие права доступа к ресурсам;

4. Обслуживающий персонал.

В связи с тем, что вход в офисное помещение закрывают с применением современной надежной двери, а все помещения оснащены сигнализацией, выведенной на диспетчерский пульт охранной организации, не представляют интереса в рамках данной работы.

В качестве метода совершенствования комплексной системы обеспечения информационной безопасности в отношении таких нарушителей необходимо реализовать установку железных решеток на окна помещений. Такое требование будет дополнительно изложено в четвертом разделе дальнейшей работы.

Учитывая специфику деятельности медицинской организации важно обратить внимание внутренним злоумышленникам.

К примеру, инсайдеры могут передать персональные данные пациентов злоумышленникам.

Другими словами, внутренними злоумышленниками информационной безопасности медицинских учреждений являются сотрудники самой организации, являющиеся легальными участниками процессов медицинской организации, а также персонал, обслуживающий аппаратно-программные комплексы или допущенный к ним в соответствии со своими служебными обязанностями [11].

Вероятность нанесения ущерба тем выше, чем более высокой квалификацией обладает сотрудник, чем на более высоком уровне иерархии информационной инфраструктуры организации он находится и чем к большему объему электронных информационных ресурсов он имеет доступ.

Главная цель, которую себе ставит внутренний злоумышленник, заключается в получении контроля над электронными информационными ресурсами медицинской организации, включая средства их обработки, хранения и предоставления, на самом высоком доступном для него уровне.

Можно выделить следующие признаки классификации внутреннего злоумышленника информационных систем медицинских учреждений:

1. Опыт и знания в профессиональной сфере.
2. Доступные ресурсы, необходимые для выполнения служебных задач.
3. Сфера функциональной деятельности.
4. Наличие мотивации действий.

Обычно, нарушители классифицируются по уровню их возможностей (т.е. по тому параметру, который им предоставляет имеющаяся в ООО «Семейная поликлиника» инфраструктура).

Выделяется четыре уровня этих возможностей (рисунок 3.1). Само разделение и категоризация злоумышленников носят иерархический характер. Другими словами, предыдущие уровни составляют некоторую часть последующих [17].

В ООО «Семейная поликлиника» важная роль должна отводиться администраторам информационной системы и ее инструментов, а также специалистам по информационной безопасности.

Они имеют высший приоритет доступа, понимают уязвимости, знают необходимые меры защиты: как превентивные, так и импульсные.

Эти сотрудники в своей работе используют не только обычное и общедоступное оборудование, но и, при необходимости, специализированное.

Важно понимать, что от работы этой категории персонала зависит информационная безопасность всей клиники.

Требуются особые процедуры, когда идет подбор, отбор и прием специалистов на должности.

Не стоит забывать и о том, что текущий срез деятельности информационных администраторов периодически обязан подвергаться контролю [17].

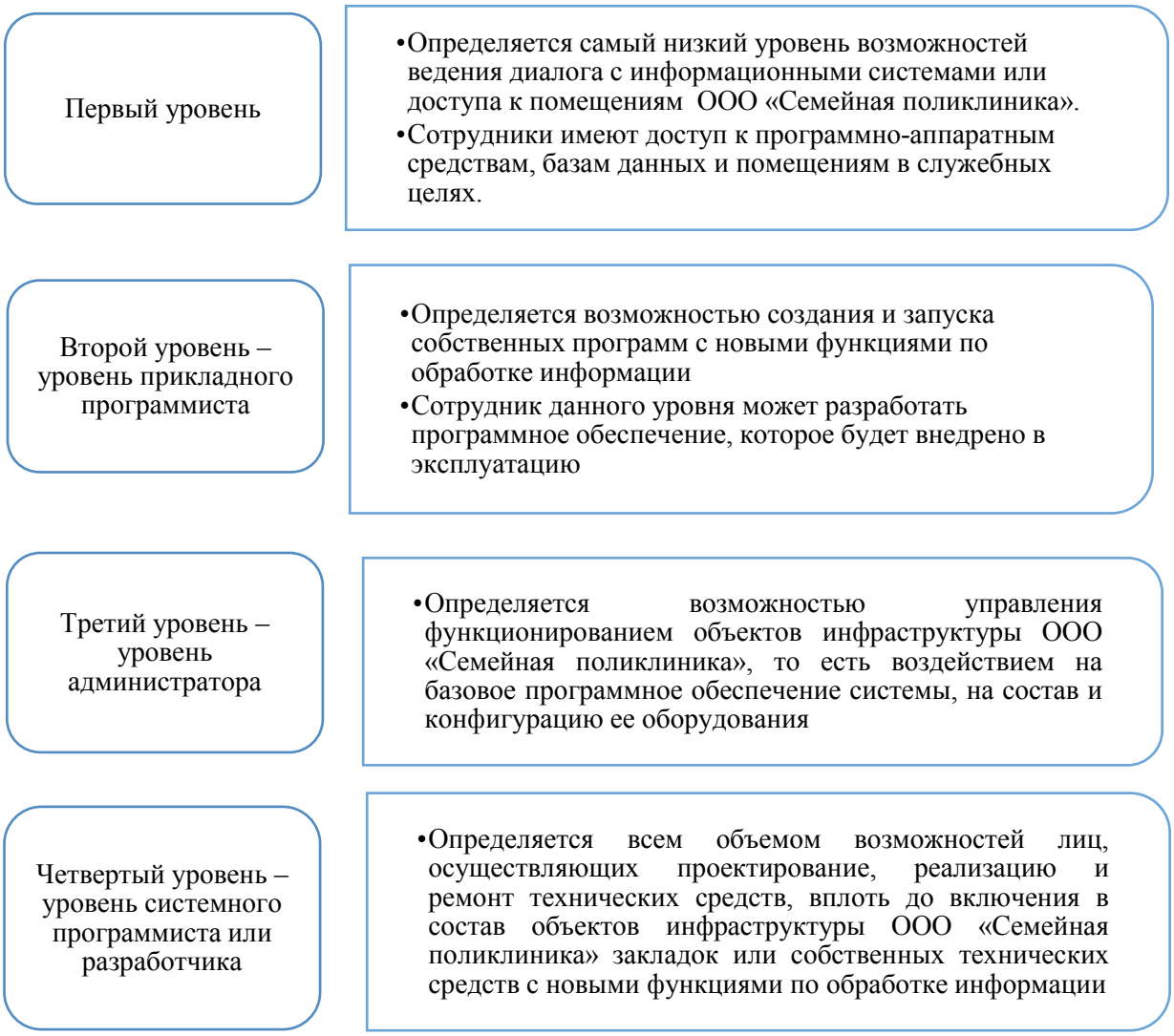

Рисунок 3.1 – Классификация нарушителей безопасности

Логичен вывод - максимально вероятные нарушители потенциально относятся к первым трем уровням классификации нарушителей безопасности.

У них есть доступ (хоть и разного допуска) к закрытым помещениям и программно-техническим средствам ООО «Семейная поликлиника».

Стоит отслеживать социальное положение и материальную обеспеченность этой группы персонала, так как они могут послужить причиной нарушения законодательства страны для получения определенного вознаграждения.

3.3 Анализ уязвимостей и угроз безопасности организации, осуществляющей медицинскую деятельность

На сегодняшний день можно выделить значительное число различных видов угроз безопасности ООО «Семейная поликлиника». Анализ научных источников показывает, что природа возникновения угроз носит либо естественный, либо искусственный характер [1].

К естественным угрозам безопасности информационной системы относят такие факторы, которые вызваны объективными обстоятельствами. Они не зависят от человека и возникают по стечению неких неблагоприятных событий. Искусственные же, наоборот, заранее продуманы определенным кругом лиц либо проявляются в результате неумышленной халатности человека.

Говоря о целях злоумышленников, которые способны нанести вред информационной безопасности инфраструктуры ООО «Семейная поликлиника», можно выделить нижеследующие:

1. Получение с целью передачи или разглашения данных о пациентах, подпадающих под категорию врачебной тайны.
2. Доступ к закрытым данным внутри информационной системы поликлиники или в соответствующих помещениях с целью последующего нарушения.
3. Попытки сбить нормальный ритм работы информационной системы: ее целостность, достоверность хранимой информации.

На основании сделанного во втором разделе работы исследования системы информационной безопасности ООО «Семейная поликлиника», а также выявленных факторов возможных нарушений можно сделать вывод: основные проблемы вытекают из распределенности (нецентрализованности) и открытости части компонентов и объектов системы. На рисунке 3.2 продемонстрированы наиболее актуальные и уязвимые места предполагаемых сетевых атак на подсистемы информационной инфраструктуры медицинского учреждения [27].

Изменение данных, циркулирующих в объектах	• Изменение данных с целью организации дезинформации или реализации информационного воздействия
Перехват сеанса взаимодействия	• Подмена компонента объекта информационной инфраструктуры ООО «Семейная поликлиника»
Парольные атаки	• Завладение паролем и логином законного компонента объекта информационной инфраструктуры ООО «Семейная поликлиника»
Анализ сетевого трафика, передаваемого между компонентами объектов	• Прослушивание каналов связи и анализ передаваемых данных между компонентами объектов информационной инфраструктуры ООО «Семейная поликлиника» для изучения топологии и архитектуры построения системы, а также получения циркулирующей информации
DDoS – атаки	• От снижения качества обслуживания легитимных пользователей до полной потери доступа легитимных пользователей к объектам информационной инфраструктуры ООО «Семейная поликлиника»
Фрод или мошенничество	• Получение конфиденциальной информации, неавторизованный доступ к ресурсам
Атаки «IP-спуфинг»	• Получение информации, циркулирующей между компонентами объекта информационной инфраструктуры ООО «Семейная поликлиника», подлог информации, корректировка передаваемой информации, внедрение вредоносной информации
Атаки на уровне приложений	• Использование портов, которым разрешен проход через межсетевой экран

Рисунок 3.2 – Перечень наиболее актуальных сетевых атак, направленных на компоненты объектов ООО «Семейная поликлиника»

Следовательно, в рамках исследования сделано предположение, что основной и наиболее востребованной проблемой является анализ уязвимостей информационного характера. Сюда, в первую очередь, входят технические угрозы (открытые стандарты, максимально расширяющие доступ). Они выявлены на всех уровнях системы и инфраструктуры исследованного объекта – ООО «Семейная поликлиника».

Несмотря на защищенность информации, передаваемой через IP-протокол, назвать его применение в медицинской организации оправданным нельзя. Такие сведения легко перехватить, невозможно гарантировать однозначной их доставки. Система (в случае соответствующего намерения злоумышленников высокого уровня) подвержена атакам вирусов, спаму, преднамеренной нагрузке на сеть (DDoS) с целью ее замораживания. Следует остановиться подробнее на вероятностно возможных угрозах:

1. «Прослушка» (анализ) сетевого трафика между модулями информационной системы поликлиники. Данное мероприятие проводится с целью получения сведений, передаваемых по каналам связи, изучения архитектуры системы безопасности ООО «Семейная поликлиника», выявления ее топологии. Главная задача – получение циркулирующей в реальном времени информации.

2. Изменение Корректировка сведений, передающихся по каналам связи внутри информационной системы поликлиники. Нарушитель, который получил доступ к механизмам передачи информации, вполне способен не просто воспользоваться ими, но и целенаправленно изменить. Таким образом он внесет элементы дезинформации, сможет осуществить определенное воздействие на данные.

3. Перехват сеанса взаимодействия (от англ. session hijacking). Угроза подразумевает подмену сессии, текущего сеанса. Изначально осуществляется аутентификация пользователя, подтверждение его полномочий, уровня доступа к элементам информационной инфраструктуры ООО «Семейная поликлиника». Злоумышленник, в ответ, переключает поток данных на новый канал, а

текущий, легитимный сеанс, разрывается. По факту, вместо реального, уполномоченного пользователя, в систему внедряется нарушитель.

Также, если взломщик использовал прокси-сервера или пиринговые сети, то определить его IP-адрес окажется невозможным (он окажется подделанным). Следовательно, получается, что внутри организации не применяется ограничение доступа на основании лимитированного спектра адресов. Такое положение дел осложняется еще и тем, что нарушитель способен запустить в систему червя, вредоносную программу, а то и вовсе сделать спам-рассылку пользователям (те, отреагировав на просьбу администратора, могут еще сильнее усугубить ситуацию – отправить злоумышленнику дополнительные данные).

4. Парольные атаки (брутфорс). Получение паролей ключевых пользователей информационной системы в ООО «Семейная поликлиника» может существенно расширить возможности взломщиков. Механизмы такого действия известны: перебор автоматический, подмена адресов, сниффинг (подслушивание).

5. Атака через сетевые порты. Так как в работе системы используется широкий набор программных средств, они связаны между собой определенными портами. Их много, они никак не экранируются и, фактически, невозможно заранее предугадать номер порта, с которого будет осуществлена атака. Выходит, что полностью их исключить невозможно (в облаке приложений). Причина в том, что в ООО «Семейная поликлиника» применяется большое количество компонент, а они, в свою очередь, обладают уязвимостями.

6. Фрод (мошенничество в сфере информационных технологий).

Основная цель применения операции фрода – получение закрытой информации (коммерческой тайны, персональных сведений) для последующей перепродажи заинтересованным персонам (конкурентам, органам контроля и т.п.). Инструментом для осуществления фрода способен стать любой циркуляр информации на физическом уровне (радиоканал, беспроводная сеть,

оптоволоконное соединение). Чтобы предотвратить подобное злоумышленническое деяние важно постоянно следить за потоками информации внутри системы. В случае ООО «Семейная поликлиника» это является невозможным на текущий момент (оборудование поставщиков услуг связи несовместимо). Проблему необходимо осмыслить, и срочно изменить ситуацию.

7. DOS – атаки. Еще один инструмент в руках мошенников. Они способны нарушить работу информационной инфраструктуры ООО «Семейная поликлиника». Цели атак перечислены ниже:

– Атаки подобного рода чреваты негативными проявлениями на уровне всей системы информации медицинского учреждения. Они могут продуцироваться как снижением качества обслуживания основной категории пользователей, так и потерей доступа всеми участниками сети. Важно отметить и то обстоятельство, что успешно проведенная атака на один из объектов инфраструктуры может негативно сказаться на работе других модулей. Для медицинского заведения такое недопустимо.

– Более того, успешная реализация DDoS мероприятия в отношении только одного компонента системы ООО «Семейная поликлиника» способно вылиться в заморозку всей сети или отдельного участка. Инфраструктура перестанет выполнять свои функции на определенное время.

8. Атаки типа «IP-спуфинг».

Так как для обмена данными между агрегатами информационной инфраструктуры медицинской организации ООО «Семейная поликлиника» необходима сеть, сведения передаются по IP-адресам.

Для нарушителя – это еще один из способов осуществить свои намерения. «IP-spoofing» – научное определение означенного действия.

Цель взломщика – выдать себя за «своего», независимо от того, где он сейчас находится физически (внутри поликлиники или за ее пределами).

Для этого он осуществляет подмену IP-адресов.

Так как для осуществления спуфинга необходим определенный диапазон адресов, он изначально должен узнать его.

В список могут входить как внутренние IP-адреса, так и внешние, имеющие право авторизации в рамках системы ООО «Семейная поликлиника».

Нарушитель может располагать инструментами, которые строят поток IP-пакетов таким образом, будто они исходят от легитимных компонентов или пользователей системы.

По факту, он обрывает связь одного из участников системы (тот может и не заметить подобного обстоятельства по ряду причин), занимает его место, получает возможность пользоваться данными организации либо их изменять.

В результате реализации «IP-спуфинга» злоумышленник наносит определенный (в некоторых обстоятельствах значительный) ущерб ООО «Семейная поликлиника». Основные способы представлены далее:

– Доступ к охраняемой информации (коммерческая, врачебная тайны, персональные сведения), которая передается внутри системы между компонентами инфраструктуры.

– Замена информации на более выгодную для нарушителя, либо внесение корректив для дезинформации и снижения эффективности системы.

– Внедрение чужеродных элементов и объектов в информационную инфраструктуру медицинской организации ООО «Семейная поликлиника».

Следовательно, можно сделать определенный вывод. Объекты информационной инфраструктуры ООО «Семейная поликлиника» находятся под угрозой воздействия определенного круга как внешних, так и внутренних факторов.

Разработка предупреждающих мер информационной безопасности – важная задача для учреждения.

Далее будет предложена модель для противостояния подобного рода угрозам с учетом ситуации внутри организации.

3.4 Разработка модели актуальных угроз безопасности объектов критической инфраструктуры организации, осуществляющей медицинскую деятельность

В дальнейшей работе в первую очередь определим актуальные угрозы информационной безопасности для объектов критической инфраструктуры медицинской организации ООО «Семейная поликлиника». Целью анализа угроз безопасности информации является определение возможных способов реализации (возникновения) угроз безопасности информации и последствий их реализации (возникновения) с учетом состава пользователей и их полномочий, программных и программно-аппаратных средств, взаимосвязей компонентов значимого объекта, взаимодействия с иными объектами критической информационной инфраструктуры, информационными системами, автоматизированными системами управления, информационно-телекоммуникационными сетями, а также особенностей функционирования значимого объекта.

Анализ угроз безопасности информации должен включать:

1. Выявление источников угроз безопасности информации и оценку возможностей (потенциала) внешних и внутренних нарушителей;
2. Анализ возможных уязвимостей значимого объекта и его программных, программно-аппаратных средств;
3. Определение возможных способов (сценариев) реализации (возникновения) угроз безопасности информации;
4. Оценку возможных последствий от реализации (возникновения) угроз безопасности информации.

В качестве исходных данных для анализа угроз безопасности информации используется банк данных угроз безопасности информации, ведение которого осуществляется ФСТЭК России в соответствии с подпунктом 21 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. № 1085.

Модель угроз безопасности информации может разрабатываться для нескольких значимых объектов, имеющих одинаковые цели создания и архитектуру, а также типовые угрозы безопасности информации. В связи с тем, что все выявленные объекты критической информационной инфраструктуры входят в состав единой локальной сети, представленной в приложение В, определим наиболее актуальные угрозы для всех выявленных объектов критической информационной инфраструктуры медицинской организации ООО «Семейная поликлиника» и представим результаты в таблице 1 Приложения Г.

По результатам анализа в дальнейшей работе будет проведена оценка возможных последствий от реализации угроз безопасности информации и категории объектов критической информационной инфраструктуры с целью дальнейшей разработки организационно-технических мер, направленные на блокирование и нейтрализацию выявленных угроз безопасности информации [28].

3.5 Определение категории выявленных объектов критической информационной инфраструктуры организации, осуществляющей медицинскую деятельность

Для того, чтобы определить попадает ли объект критической информационной инфраструктуры медицинской организации ООО «Семейная поликлиника» в соответствующие категории значимости, следует учесть выявленные критические процессы и объекты на ряду с разработанной моделью угроз безопасности объектов критической инфраструктуры и выявленными факторами активности потенциального злоумышленника. Подробный алгоритм определения категорий значимых объектов критической информационной инфраструктуры изложен в Постановлении Правительства РФ от 8 февраля 2018 г. № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов

критической информационной инфраструктуры Российской Федерации и их значений».

В качестве примера на рисунке 3.3 представлено схематичное изображение определения категории объекта критической информационной инфраструктуры. Наименования ИС1, Ис2, АСУ1, АСУ2, как и вся схема, представленная на рисунке 3.3, носят ознакомительный характер, отображающий связь значений показателей из Постановления Правительства РФ № 127 с наименованиями объектов КИИ.

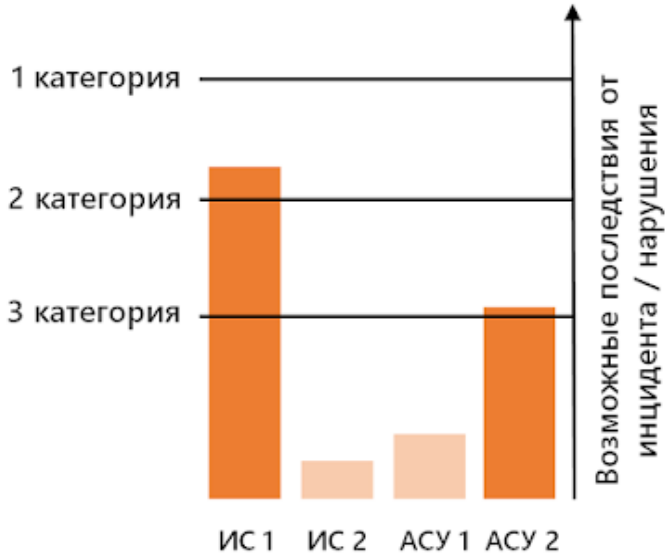

Рисунок 3.3 – Схематичное изображение определения категории объекта критической информационной инфраструктуры

Очевидно, что если объект критической информационной инфраструктуры автоматизирует или предоставляет информацию для обеспечения определенного процесса медицинской организации ООО «Семейная поликлиника», то ущерб от инцидента на объекте не может превышать максимального ущерба от нарушения всего процесса, включающего как автоматизированную, так и неавтоматизированную деятельность.

Одновременно, очевидно, что скорость реакции на сбои или непредсказуемое поведение информационной инфраструктуры напрямую влияет на степень потенциального ущерба от чрезвычайного происшествия. Если реакция займет несколько секунд – последствия не будут существенными,

независимо от действий злоумышленника или стечения стихийных обстоятельств. После преодоления некоторого разумного лимита ущерб начнет нарастать мультипликативно. Тем не мене, меры принимать все-равно придется, пусть и с большими затратами.

Таким образом, в рамках оценки категории объекта критической информационной инфраструктуры необходимо учитывать следующий факторы:

1. Сможет ли ущерб он нарушения процесса на сколь угодно долгое время достичь показателя значимости критической информационной инфраструктуры.
2. Если в принципе может достичь показателей значимости, то в каких промежутках попадает в какую категорию (например, если деятельность будет нарушена на 1-10 дней – то потенциальный ущерб попадет в 3 категорию, если на 10-30 то во 2 категорию).

При этом для упрощения процесса категорирования ущерб можно оценить исходя из следующих составляющих:

1. Упущенная выгода.
2. Штрафы, пени, неустойки и т.п.
3. Дополнительные затраты на персонал.
4. Дополнительные затраты на оборудование, материалы, энергию и т.п.
5. Судебные издержки.
6. Дополнительные представительские расходы.

Оценим значимость объектов критической информационной инфраструктуры медицинской организации ООО «Семейная поликлиника» в соответствие с перечнем показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации, представленном в Постановление Правительства РФ № 127 от 8 февраля 2018 г. При этом в рамках оценки допустим объединение объектов критической информационной инфраструктуры исследуемой медицинской организации

ООО «Семейная поликлиника», представленных в пункте 2.3, в следующие подгруппы:

1. ИС, связанные с обслуживанием клиентов - информационные системы, обрабатывающие персональные данные клиентов.

2. ИС, связанные с обслуживанием сотрудников - информационные системы, обрабатывающие персональные сотрудников.

3. АСУ пожаротушением - автоматизированная система управления пожаротушением.

4. АСУ оборудованием - автоматизированная система управления рентгеном, томографом и др.

5. Корпоративная сеть.

Результат оценки представлен в таблице 1 Приложения Д. По результатам оценки было определено отсутствие необходимости отнесения корпоративной сети к объектам критической информационной инфраструктуры медицинской организации. Информационные системы, связанные с обслуживанием клиентов и сотрудников, а также АСУ по работе с оборудованием и пожаротушением отнесены к 3 категории значимости.

3.6 Выводы по разделу 3

Таким образом, исходя из проведенного исследования вопроса категорирования объектов критической информационной инфраструктуры Российской Федерации на примере медицинской организации ООО «Семейная поликлиника» были выявлены критические процессы, определены объекты критической информационной инфраструктуры ООО «Семейная поликлиника», проведена оценка факторов активности потенциального злоумышленника, а также разработана модель угроз безопасности объектов критической инфраструктуры медицинского учреждения.

По результату проведенного исследования были определены категории значимых объектов критической информационной инфраструктуры медицинской организации ООО «Семейная поликлиника» в соответствие с

Постановлением Правительства РФ № 127 от 8 февраля 2018 г. В дальнейшей работе необходимо разработать рекомендаций по совершенствованию комплексной системы информационной безопасности медицинской организации ООО «Семейная поликлиника» на основании определенных категорий значимости объектов информационной инфраструктуры медицинского учреждения.

4. СОВЕРШЕНСТВОВАНИЕ КОМПЛЕКСНОЙ СИСТЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ, ОСУЩЕСТВЛЯЮЩЕЙ МЕДИЦИНСКУЮ ДЕЯТЕЛЬНОСТЬ

Обеспечение комплексной безопасности является необходимым условием безопасного функционирования любого медицинского учреждения как субъекта критической инфраструктуры. Необходимый уровень безопасности должен обеспечиваться за счет организационных, технических, а также инженерных мер и методов защиты.

В соответствие с Приказом ФСТЭК от 25.12.2017 №239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» для значимых объектов критической инфраструктуры в зависимости от категории значимости и угроз безопасности информации должны быть определены и внедрены организационные и технические меры. Для 3 класса значимости предусмотрен следующий перечень:

1. Идентификация и аутентификация.
2. Управление доступом.
3. Защита машинных носителей информации.
4. Аудит безопасности.
5. Антивирусная защита.
6. Обеспечение целостности.
7. Обеспечение доступности.
8. Защита технических средств и систем.
9. Защита информационной (автоматизированной) системы и ее компонентов.
10. Планирование мероприятий по обеспечению безопасности.
11. Управление конфигурацией.
12. Управление обновлениями программного обеспечения.

13. Реагирование на компьютерные инциденты.

14. Обеспечение действий в нештатных ситуациях.

15. Информирование и обучение персонала.

Таким образом, в целях соответствия нормативным документам комплексная система обеспечения информационной безопасности медицинской организации ООО «Семейная поликлиника» должна:

1. Предотвращать несанкционированный доступ к информации и (или) передачу ее лицам, не имеющим права на доступ к информации.

2. Обеспечивать своевременное обнаружение фактов несанкционированного доступа к информации.

3. Обеспечивать предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации.

4. Обеспечивать недопущение воздействия на технические и программные средства обработки информации, в результате которых нарушается их функционирование.

5. Обеспечивать незамедлительное восстановление информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней.

6. Обеспечивать постоянный контроль за обеспечением уровня защищенности информации.

7. Обеспечивать защиту информации при ее передаче по информационно-телекоммуникационным сетям.

8. Обеспечивать применение сертифицированных по требованиям безопасности информации средств защиты информации.

9. Обеспечивать защиту информации в ходе эксплуатации иной информационной системы.

10. Обеспечивать обязательность учета и регистрации действий и идентификации участников, связанных с обработкой персональных данных в иных информационных системах.

11. Обеспечивать соблюдение следующих организационных мер:

- формирование требований к защите информации, содержащейся в иной информационной системе;

- разработка и внедрение системы (подсистемы) защиты информации иной информационной системы;

- минимизация состава обрабатываемых персональных данных, необходимых для решения возлагаемых на иные информационные системы задач;

- декларирование и соответствие порядка обработки персональных данных целям их обработки;

- определение информационного запроса как преимущественного способа получения в иных информационных системах сведений об объекте (субъекте) персональных данных;

- хранение персональных данных в электронном виде в информационных системах по месту возникновения таких данных.

12. Соответствовать требованиям по обеспечению целостности, устойчивости функционирования и безопасности информационных систем общего пользования, утвержденным Министерством связи и массовых коммуникаций Российской Федерации, а также требованиям, утвержденным Федеральной службой безопасности Российской Федерации совместно с Федеральной службой по техническому и экспортному контролю.

Меры, выполнение которых необходимо для обеспечения безопасности медицинской организации ООО «Семейная поликлиника», определяются конкретными законодательными документами.

При определении мер следует учитывать возможные угрозы, связанные с соответствующим категории объекта уровнем потенциалом источника, а также соотношение категории значимости и требуемого класса средств защиты информации.

Данная связка представлена в таблице 4.1.

Таблица 4.1 - Оценка требуемого класса средств защиты информации

Категория объекта КИИ	Потенциал источника угроз, который следует рассматривать при выборе мер	Уровень контроля отсутствия НДВ	Требуемый класс СЗИ
1 категория	Высокий	Не ниже 4 уровня	Не ниже 4 класса
2 категория	Базовый усиленный	Не ниже 4 уровня	Не ниже 5 класса
3 категория	Базовый	-	Не ниже 6 класса

В рамках совершенствования комплексной системы обеспечения информационной безопасности медицинской организации ООО «Семейная поликлиника» необходимо также вносить соответствующие изменения в политику информационной безопасности, представляющую собой самый важный документ в системе управления информационной безопасностью медицинского учреждения. Политика ИБ должна полностью соответствовать требованиям международного стандарта ISO 27002. В Российской Федерации действует государственный общероссийский стандарт (ГОСТ) Р ИСО/МЭК 27002-2012 [2].

Меры и методы обеспечения безопасности информации выявленных значимых объектов критической инфраструктуры ООО «Семейная поликлиника» должны быть направлены на нейтрализацию указанных в 3 главе угроз безопасности информации и подразделяться следующим образом.

1. Комплекс организационных мер и методов обеспечения информационной безопасности критической инфраструктуры медицинского учреждения.

Организационные меры играют существенную роль в создании надежного механизма защиты объектов критической инфраструктуры ООО «Семейная поликлиника». К текущему моменту осуществлены мероприятия обучающего характера. Сотрудники были проинструктированы о мерах безопасности, защите данных, предполагаемых действиях в случае обнаружения неполадок или сбоев в информационной системе. Это позволяет

говорить о том, что общий уровень информационной безопасности в ООО «Семейная поликлиника» растет. Вместе с тем, осуществляется контроль осведомленности персонала об угрозах безопасности информации и о правилах безопасной работы.

Однако в положениях о подразделениях и должностных инструкциях руководителей и сотрудников медицинской организации ООО «Семейная поликлиника» пункты об ответственности за передачу, а также разглашение либо утрату атрибутов разграничения доступа не предусмотрено.

На сегодняшний день в соответствие с ФЗ № 239 уже разработаны в медицинской организации ООО «Семейная поликлиника» некоторые политики идентификации и аутентификации, аудита безопасности, политика управления доступом, защиты носителей информации, политика об антивирусной защите, обеспечения целостности и доступности, а также ряд других политик безопасности

В части проведения аудита безопасности нареканий нет - аудит проводится на периодической основе сторонней организацией, в рамках которого происходит инвентаризация информационных ресурсов, регистрация событий безопасности, мониторинг безопасности, а также проверяется реагирование на сбои при регистрации событий безопасности.

Среди организационных мер по защите выявленных значимых объектов критической инфраструктуры ООО «Семейная поликлиника» необходимо следующие направления проработать более подробней:

– размещение технических средств (отдельно уделить внимание в части размещения устройств вывода информации, чтобы исключить возможность несанкционированного просмотра);

– порядок работы со носителями информации и мобильными устройствами;

– защита информации от несанкционированного доступа;

– порядок работы администратора безопасности;

– порядок и правила использования паролей пользователей.

Документы, регламентирующие организационные мероприятия по защите выявленных значимых объектов критической инфраструктуры медицинской организации ООО «Семейная поликлиника», можно определить следующим перечнем:

– перечень сотрудников, имеющих допуск к работе с выявленными значимыми объектами;

– положение о защите значимых объектов критической инфраструктуры медицинского учреждения;

– приказ о выделении помещений для защиты значимых объектов критической инфраструктуры медицинского учреждения;

2. Комплекс программно-аппаратных мер и методов обеспечения информационной безопасности в части технической и физической защиты.

На текущий момент установлена охранная и пожарная сигнализация, двери закрываются на замок, однако организация безопасности контролируемой зоны соответствующей службой обеспечена не полностью. Все точки входа / выхода и въезда / выезда из здания медицинского учреждения, в которых функционируют значимые объекты критической инфраструктуры, оборудованы системой контроля и управления доступом, системами оповещения и видеомониторинга, однако не оснащенными постами охраны и турникетами, а на окнах кабинетов не установлены решетки.

Вместе с тем существующая система не предусматривает разграничение предметных зон, позволяющих сопоставлять функциональные обязанности сотрудников и категорию значимость объекта критической информационной инфраструктуры.

По результатам проведенного анализа в 3 главе, перечислим требуемые программно-аппаратные средства значимых объектов критической инфраструктуры следующим списком:

– средство защиты информации от НСД;

– антивирусное средство;

– средство анализа защищённости.

Документы, регламентирующие технические мероприятия по защите значимых объектов критической инфраструктуры медицинской организации ООО «Семейная поликлиника», можно определить следующим перечнем: план мероприятий по обеспечению защиты информации; план действий в нештатных ситуациях; журнал учета и хранения носителей; акт установки средств защиты информации; акт списания и уничтожения электронных носителей; акт уничтожения документов.

4.1 Определение оптимального комплекса организационных мер и методов обеспечения информационной безопасности

Организационные меры по размещению ТС в медицинской организации ООО «Семейная поликлиника», разработанные в данной работе:

1. Все технические средства значимых объектов критической инфраструктуры расположены в помещениях в пределах контролируемых зон.
2. Предусмотрены организационные меры, которые создают ограничения к несанкционированному доступу к техническим средствам значимых объектов критической инфраструктуры (режим доступа в помещения, порядок допуска к работе с техническими средствами, опечатывание корпусов и мест подключения периферийных устройств к основным техническим средствам обработки).
3. Предусмотрены организационные меры, которые создают ограничения к несанкционированному доступу к АРМ (режим доступа в помещения, порядок допуска к работе с АРМ).
4. Предусмотрены организационные меры, которые создают ограничения к несанкционированному доступу к СрЗИ (определен порядок допуска к работе с СрЗИ, определен порядок их использования).
5. При размещении технических средств, использующих СрЗИ, учтены рекомендации на данные средства.
6. Расположение технических средств, установленных для вывода защищаемой информации на печать, реализовано с учетом наибольшего

затруднения визуального просмотра лицами, не имеющими допуска к этой информации.

Все находящиеся на хранении и в обращении съемные носители медицинской организации ООО «Семейная поликлиника» должны учитываться в Журнале учета носителей. Каждый носитель с записанными должен иметь этикетку, на которой указывается метка съемного носителя и гриф.

Пользователи значимых объектов критической инфраструктуры для выполнения работ получают учтенный съемный носитель от администратора безопасности. При получении вносятся соответствующие записи в Журнале учета.

В помещениях, содержащих ТС или другие компоненты значимых объектов критической инфраструктуры, не допускается использование мобильных устройств.

Администратор безопасности медицинской организации ООО «Семейная поликлиника» назначается на высшем уровне если есть необходимость, то на среднем и нижнем уровнях.

Администратор безопасности должен обладать знаниями по настройке и использованию средств защиты информации, которые применяются к значимым объектам критической инфраструктуры, в соответствии документацией которая входит в их поставку, также требованиям и выписками из заключений, которые определяют порядок их использования.

Администратор безопасности ведет журналы учета работы пользователей и печати пользователями документов, идентификаторов и паролей доступа пользователей к ТС, идентификаторов и паролей доступа администратора к ТС, учета неисправностей и попыток реализации угроз безопасности.

Администратор информационной безопасности контролирует соблюдение политики безопасности и соблюдение соответствующих приказов. А так же на него возложена обязанность за контролем выполнения мероприятий по обеспечению защиты информации, он же осуществляет

резервное копирования и восстановления программного обеспечения при различных сбоях и нештатных ситуациях.

При использовании паролей в значимых объектах критической инфраструктуры ООО «Семейная поликлиника» необходимо выполнять следующие правила:

1. Пароли необходимо менять с установленной периодичностью в соответствии с требованиями организационно-распорядительного документа.
2. Пароль должен иметь не менее 6 символов и содержать буквенные и цифровые символы.
3. Обязательно применение индивидуальных паролей.
4. Применение групповых паролей не допускается.
5. Для предотвращения повторного использования паролей необходимо вести учет (запись) за предыдущие 12 месяцев.

При использовании паролей необходимо ввести запрет на следующие действия: использования в качестве пароля своего ФИО, даты рождения, клички собаки и т. п.; использования в качестве пароля легко вычисляемых сочетаний символов, а также общепринятых сокращений.

4.2 Определение оптимального комплекса программно-аппаратных мер и методов обеспечения информационной безопасности в части технической и физической защиты

В первую очередь необходимо обеспечить наличие решеток на окнах защищаемых помещений и сотрудника службы безопасности, организующего учет лиц, допущенных к помещениям медицинского учреждения, и оперативно реагирующего на срабатывания охранной сигнализации. Вместе с тем, такой сотрудник должен отслеживать передвижение посторонних лиц по защищаемой территории при помощи внутреннего и наружного видеонаблюдения.

Система контроля управления доступом медицинской организации ООО «Семейная поликлиника» должна содержать ряд предметных зон, позволяющих сопоставлять функциональные обязанности сотрудника и категорию

значимости объектов критической инфраструктуры, к которым сотрудник может получить доступ. Целесообразно включить в учетную форму следующие зоны:

1. Зона штатных функциональных обязанностей работника, при реализации которых используются значимые объекты критической инфраструктуры (согласно утвержденной должностной инструкции).

2. Зона изменений и дополнений, внесенных в функциональные обязанности работника.

Такой подход позволит не только дополнить защиту периметра объектов критической информационной инфраструктуры, но и организовать эшелонированную защиту систем. Анализ осуществляется сравнением содержания записей в зонах и индексов известных сотруднику, т.е. ведется поиск несоответствия.

Вместе с тем, необходимо реализовать программно-аппаратную защиту значимых объектов критической информационной инфраструктуры ООО «Семейная поликлиника».

В целях организации идентификации и аутентификации пользователей и инициируемых ими процессов, устройств, а также других аспектов идентификации и аутентификации следует использовать системы защиты информации от несанкционированного доступа. Такая система позволит обеспечить управление учетными записями пользователей, разделение полномочий (ролей) пользователей, назначение минимально необходимых прав и привилегий и другие аспекты управления доступом.

Методика сравнительного анализа СЗИ от НСД «Аккорд-Win64» и «Страж NT 4.0» приводится ниже. Критериями для сравнительного анализа в настоящей работе выбраны следующие технические характеристики систем защиты информации от несанкционированного доступа:

1. Уровень контроля НДВ и СВТ.
2. Дополнительные аппаратные требования.
3. Стоимость лицензии.

Указанные технические характеристики для выбранных СЗИ от НСД приводятся в таблице 4.2.

Таблица 4.2 - Сравнительный анализ СЗИ от НСД

Критерии сравнения	Аккорд-Win64	Страж NT 4.0
РД НДВ	4 уровень контроля отсутствия НДВ	2 уровень контроля отсутствия НДВ
РД СВТ	5 класс защищенности СВТ от НСД	3 класс защищенности СВТ от НСД
Требования к серверу безопасности системы	Windows Server 2008 R2 и выше, CPU x64, 2 ядра или больше, RAM 4GB, HDD 80 GB, LAN 100Mb	нет
Требования к АРМ пользователей	Конфигурация АРМ определяется требованиями к соответствующей ОС	Конфигурация АРМ определяется требованиями к соответствующей ОС
Стоимость лицензии	8800 руб.	7500 руб.

В результате проведенного анализа была выбрана система защиты информации (СЗИ) от несанкционированного доступа «Страж NT 4.0».

Такой выбор был осуществлен по причине сравнительно небольшой цены и подходящих технических характеристик. СЗИ «Страж NT 4.0» - предназначено для комплексной защиты информации от несанкционированного доступа в локальных сетях и автономных автоматизированных информационных системах.

Система защиты информации от несанкционированного доступа «Страж NT 4.0» сертифицирована в Системе сертификации средств защиты информации. Сертификат ФСТЭК России № 3553 (выдан 20.04.2016, действителен до 20.04.2024) удостоверяет, что комплекс СЗИ НСД «Страж NT 4.0» соответствует требованиям руководящих документов по 3-му уровню контроля отсутствия недекларированных возможностей и по 3 классу руководящих документов (РД) СВТ, то есть подходит к защищаемым объектам

критической информационной инфраструктуры медицинской организации ООО «Семейная поликлиника».

Функционал СЗИ «Страж NT 4.0» можно представить следующим перечнем:

1. Двухфакторная аутентификация до загрузки операционной системы (в том числе и для виртуальной среды) с использованием аппаратных идентификаторов.
2. Дискреционный принцип контроля доступа к ресурсам системы.
3. Мандатный принцип контроля доступа к ресурсам системы.
4. Создание замкнутой программной среды пользователя, позволяющей ему запуск только разрешенных приложений.
5. Регистрация событий безопасности, в том числе и действий администратора.
6. Маркировка выдаваемых на печать документов независимо от печатающего их приложения.
7. Контроль целостности защищаемых ресурсов системы и компонентов системы защиты информации.
8. Управление пользователями.
9. Управление носителями информации.
10. Управление устройствами.
11. Тестирование системы защиты информации.

Особое внимание следует уделить вопросу идентификации и аутентификации доступа пользователей в систему, которые регламентируются работой СрЗИ НСД «Страж NT 4.0» (таблица 4.3).

Таблица 4.3 - Разграничение прав доступа

Действия	Администратор безопасности	Пользователь
Настройка и установка СрЗИ	+	-
Создание и блокирование пользователей	+	-
Создание и редактирование групп пользователей	+	-
Настройка подключения ПК и других	+	-

сетевых устройств к сети		
Доступ к серверу	+	-

Продолжение таблицы 4.3

Действия	Администратор безопасности	Пользователь
Настройка прав доступа к каталогам и разделам FTP	+	-
Доступ к сети Интернет	+	+
Возможность скачивания файлов из сети Интернет	+	-
Запись данных	+	+
Изменение данных	+	+
Удаление данных	+	+
Установка ПО	+	-
Запись системных данных	+	-
Изменение системных данных	+	-
Удаление системных данных	+	-
Подключение внешних носителей	+	+

Антивирусная защита должна обеспечивать защиту самих объектов КИИ, а также электронной почты, иных сервисов и обновление баз данных признаков вредоносных компьютерных программ.

Критериями для сравнительного анализа антивирусных систем в настоящей работе выбраны технические характеристики, представленные в таблице 4.4.

Таблица 4.4 - Сравнительный анализ антивирусных решений

Критерии сравнения	Kaspersky Endpoint Security 10	Dr.Web Enterprise Security Suite	ESET NOD32 Secure Enterprise Pack
Увеличение времени копирования файлов	29%	23%	24%
Снижение общего уровня быстродействия ПК	36%	12%	27%
Увеличение времени загрузки системы	20%	26%	25%
Увеличение времени установки/удаления приложений	59%	36%	30%

Объем занимаемой оперативной памяти	149 Мб	102 Мб	168 Мб
Размер базы сигнатур	60 Мб	30 Мб	125 Мб
Сетевой трафик за сутки	15 Мб	2 Мб	4 Мб

Из трех рассматриваемых вариантов Dr.Web Enterprise Security Suite оказывает минимальное влияние на работу системы, а также обеспечивает наименьшую нагрузку на сеть, что послужило ключевыми преимуществами в рамках выбора антивирусной системы.

Вместе с тем, рекомендация по выбору Dr.Web обусловлена тем, что в отличии от большинства конкурирующих решений программные продукты Dr.Web имеют сертификаты соответствия ФСТЭК России и ФСБ России.

Кроме того, компания "Доктор Веб" имеет лицензию Министерства обороны России на деятельность в области создания средств защиты информации.

В качестве конкретного программного продукта был выбран Dr.Web Enterprise Security Suite, представляющий собой комплекс продуктов Dr.Web и включающий элементы защиты всех узлов корпоративной сети, а также единый центр управления для большинства из них.

Сертификат ФСТЭК России № 3509 действителен до 27.01.2024 года и удостоверяет, что Dr.Web Enterprise Security Suite соответствует требованиям руководящих документов по 2 уровню контроля отсутствия недекларированных возможностей, то есть подходит для защиты объектов критической информационной инфраструктуры медицинского учреждения.

Аппаратно-программный комплекс обнаружения компьютерных атак должен обеспечивать выявление компьютерных инцидентов, анализ и информирование о компьютерных инцидентах, а также принятие мер по предотвращению и устранение последствий компьютерных инцидентов.

В качестве ключевого критерия для выбора аппаратно-программного комплекса обнаружения компьютерных атак в настоящей работе был выбран экономический эффект, получаемый от экономии на стоимости АПК.

В таблице 4.5 представлен сравнительный анализ АПК.

Таким образом, рекомендуется использование аппаратно-программного комплекса обнаружения компьютерных атак «Аргус» версии 1.6. Аппаратно-программный комплекс обнаружения компьютерных атак "Аргус", версия 1.6" сертифицирован ФСТЭК № 4048 до 19.12.2023 на соответствие ТУ и 4 уровню РД НДВ.

Таблица 4.5 - Сравнительный анализ АПК

Критерии сравнения	Организация - разработчик	Сертификат ФСТЭК	Стоимость, руб
Аргус, версия 1.6	Центр Специальной Системотехники	№ 2487	22000
Детектор атак «Континент»	ООО «Код Безопасности»	№ 3008	38000
Форпост, версия 2.0	РНТ	№ 2845	27500

АПК «Аргус» версии 1.6 имеет встроенные пользовательские интерфейсы для анализа событий ИБ, подготовки отчетов операторами и администраторами Комплекса. Вместе с тем АПК «Аргус» позволяет выявлять подозрительные воздействия и попытки проникновения в сеть.

В результате данного анализа структура средств обеспечения информационной безопасности данной организации может быть представлена в виде схемы, изображенной на рисунке 4.1.

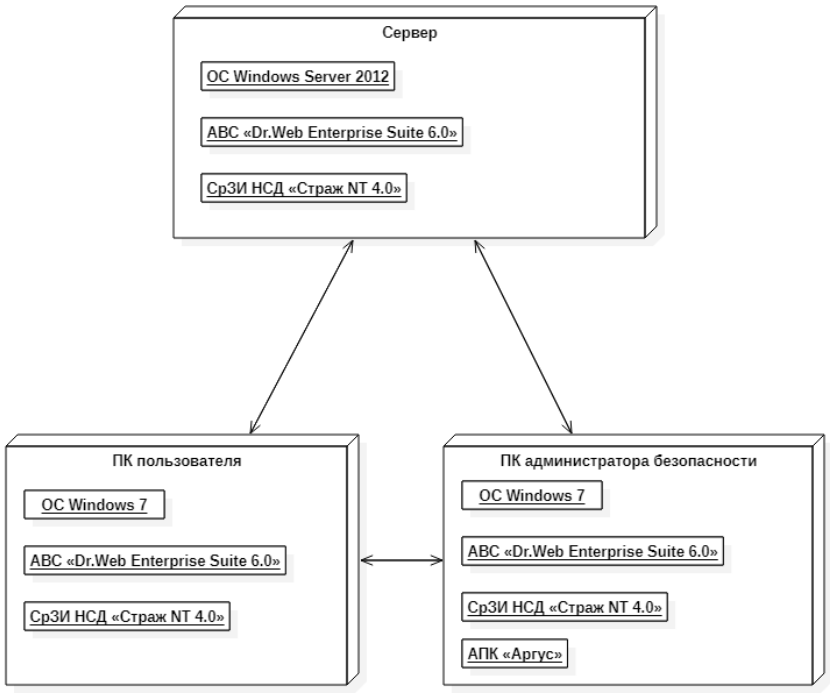

Рисунок 4.1 - Диаграмма средств обеспечения информационной безопасности

В данном разделе был определен оптимальный комплекс программно-аппаратных мер и методов обеспечения информационной безопасности в части технической и физической защиты информации.

4.3 Разработка мер защиты информации в целях нейтрализации выявленных актуальных угроз

В таблице 4.6 приведены меры защиты информации в целях нейтрализации выявленных угроз значимых объектах критической информационной инфраструктуры медицинской организации ООО «Семейная поликлиника».

Таблица 4.6 - Меры защиты информации в целях нейтрализации выявленных угроз значимых объектах КИИ ООО «Семейная поликлиника»

Наименование угрозы	Меры по противодействию угрозе	
	Технические и физические	Организационные
Угрозы значимых объектов критической информационной инфраструктуры путем физического доступа		
Кража, модификация, уничтожение информации	СрЗИ НСД «Страж NT 4.0», система контроля	Инструкции персоналу, обязательство о

	управления доступом, сотрудник СБ, средства физического предотвращения проникновения	неразглашении, размещение ТС в соответствии с политикой безопасности, ограничение использования внешних носителей, установка сертифицированного ПО
Несанкционированное отключение средств защиты	СрЗИ НСД «Страж NT 4.0», система контроля управления доступом, сотрудник СБ, средства физического предотвращения проникновения	Соблюдение порядка доступа к работе с СрЗИ, соблюдение порядка использования паролей
Угроза внедрения агентов в число персонала системы	-	Первичная и периодическая проверка сотрудников (аудит безопасности)
Угроза разглашения, передачи или утраты атрибутов разграничения доступа	-	Инструкции персоналу, обязательство о неразглашении, соблюдение порядка использования паролей

Продолжение таблицы 4.6

Наименование угрозы	Меры по противодействию угрозе	
	Технические и физические	Организационные
Угрозы значимых объектов критической информационной инфраструктуры путем физического доступа		
Угроза вывода из строя подсистем обеспечения функционирования сети.	Система контроля управления доступом, сотрудник СБ, средства физического предотвращения проникновения	Инструкции персоналу
Угроза несанкционированного использования терминалов пользователей, имеющих уникальные физические характеристики, такие как номер рабочей станции в сети, физический адрес, адрес в системе связи, аппаратный	Система контроля управления доступом, сотрудник СБ, средства физического предотвращения проникновения	Инструкции персоналу, обязательство о неразглашении, размещение ТС в соответствии с политикой безопасности, обязательная идентификация пользователей
Угрозы значимых объектов критической информационной инфраструктуры с применением		

программных и программно-аппаратных средств		
Угроза внедрения программных "закладок" и "вирусов"	СрЗИ НСД «Страж NT 4.0», АВС. Dr.Web Enterprise Security Suite 6.0, АПК «Аргус»	Инструкции персоналу, ограничение использования внешних носителей, ведение Журнала учета носителей и использования сети Интернет, установка сертифицированного ПО
Угроза незаконного получения паролей и других реквизитов разграничения доступа с дальнейшим их использованием	СрЗИ НСД «Страж NT 4.0», АПК «Аргус»	Инструкции персоналу, периодическая смена паролей, ограничение использования внешних носителей, установка сертифицированного ПО, соблюдение порядка использования паролей
Угроза реализации скрытого канала передачи данных	СрЗИ НСД «Страж NT 4.0»,	Первичная и периодическая проверка сотрудников СБ
Угроза перехвата конфиденциальной информации по сети	СрЗИ НСД «Страж NT 4.0», АПК «Аргус»	Инструкции персоналу

Условные обозначения представлены ниже:

АВС «Dr.Web Enterprise Suite 6.0»

СрЗИ НСД «Страж NT 4.0»

АПК «Аргус»

На рисунках приложений Б и В приведены схемы размещения предлагаемых средств обеспечения информационной безопасности значимых объектов критической информационной инфраструктуры медицинской организации ООО «Семейная поликлиника».

4.4 Выводы по разделу 4

Таким образом, на основании проведенного категорирования и приказа № 239 от 25 декабря 2017 "Об утверждении формы акта проверки, составляемого по итогам проведения государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации" был предложен проект совершенствования комплексной системы обеспечения информационной безопасности медицинской организации ООО «Семейная поликлиника». Предложенный проект содержит оптимальные комплексы организационных, технических и программно-аппаратных мер и методов обеспечения информационной безопасности, внедрение которых позволяет нейтрализовать выявленные актуальные угрозы безопасности медицинской организации ООО «Семейная поликлиника».

ЗАКЛЮЧЕНИЕ

В данной работе было проведено исследование вопроса обеспечения информационной безопасности критической информационной инфраструктуры, на основании которого можно сделать вывод о широком перечне уязвимостей и угроз информационной безопасности применительно к медицинским организациям. В работе были проанализированы ключевые аспекты ФЗ № 187 и определены принципы обеспечения безопасности критической информационной инфраструктуры, на основании чего был сделан вывод о необходимости повышения защищенности критических информационных инфраструктур, в частности медицинского учреждения.

Вместе с тем в работе были выявлены критические процессы, определены объекты критической информационной инфраструктуры медицинской организации ООО «Семейная поликлиника», проведена оценка факторов активности потенциального злоумышленника, а также разработана модель угроз безопасности объектов критической инфраструктуры медицинского учреждения. По результату проведенного анализа была проведена оценка категорий значимых объектов критической информационной инфраструктуры ООО «Семейная поликлиника» в соответствие с Постановлением Правительства РФ № 127 от 8 февраля 2018 г.

На основании проведенного категорирования и приказа № 239 от 25 декабря 2017 "Об утверждении формы акта проверки, составляемого по итогам проведения государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации" был предложен проект совершенствования комплексной системы обеспечения информационной безопасности медицинской организации ООО «Семейная поликлиника». Предложенный проект содержит оптимальные комплексы организационных, технических и программно-аппаратных мер и методов обеспечения информационной безопасности, внедрение которых позволяет нейтрализовать выявленные актуальные угрозы безопасности медицинской организации ООО «Семейная поликлиника».

Таким образом в результате работы были исследованы организационно-правовое и инженерно-техническое направления обеспечения информационной безопасности, подобраны меры и методы обеспечения комплексной безопасности в целях нейтрализации угроз, определенных в 3 главе, а также построены схемы размещения средств защиты информации.

Полученные результаты могут быть использованы государственными и коммерческими медицинскими организациями для проектирования современных комплексных систем защиты информации, учитывающих требования закона № 187-ФЗ, а также других нормативных документов в отношении обработки данных на субъектах критической информационной инфраструктуры.

СПИСОК ИСПОЛЬЗУЕМОЙ ЛИТЕРАТУРЫ

Нормативно-правовые акты

1. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения М.: Стандартинформ, 2008 [Электронный ресурс] : справочная правовая система: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=EXP&n=418509#06367720451532759 (Дата обращения: 20.11.2019).

2. ГОСТ Р ИСО/МЭК 27002-2012. Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности [Электронный ресурс] : сайт Федерального агентства по техническому регулированию и метрологии: http://protect.gost.ru/document.aspx?control=7&id=183918 (Дата обращения: 20.11.2019).

3. О безопасности критической информационной инфраструктуры Российской Федерации: Федеральный закон (от 26.07.2017 № 187-ФЗ) [Электронный ресурс] : сайт Президента Российской Федерации: http://www.kremlin.ru/acts/bank/42489 (Дата обращения: 20.11.2019).

4. О внесении изменений в Положение о ФСТЭК: Указ Президента Российской Федерации (от 25.11.2017 г. № 569) [Электронный ресурс] : сайт Федерального агентства по техническому регулированию и метрологии: http://protect.gost.ru/document.aspx?control=7&id=183918 (Дата обращения: 20.11.2019).

5. О внесении изменений в регламент ФСТЭК: Приказ ФСТЭК (от 26.04.2018 №72) [Электронный ресурс] : сайт Федеральной службы по техническому и экспортному контролю: https://fstec.ru/index?id=1596:prikaz-fstek-rossii-ot-26-aprelya-2018-g-n-72 (Дата обращения: 20.11.2019).

6. Об информации, информационных технологиях и о защите информации: Федеральный Закон (от 27 июля 2006 г. № 149-ФЗ) [Электронный ресурс]: справочная правовая система: http://www.consultant.ru/document/cons_doc_LAW_61798/ (Дата обращения: 20.11.2019).

7. Об утверждении порядка ведения реестра значимых объектов критической информационной инфраструктуры Российской Федерации: Приказ ФСТЭК России (от 06.12.2017 № 227) [Электронный ресурс] : сайт Федеральной службы по техническому и экспортному контролю: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/1587-prikaz-fstek-rossii-ot-6-dekabrya-2017-g-n-227 (Дата обращения: 20.11.2019).

8. Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений: Постановление Правительства РФ (от 8 февраля 2018 г. № 127) [Электронный ресурс] : информационно-правовой портал: http://www.garant.ru/products/ipo/prime/doc/71776120/ (Дата обращения: 20.11.2019).

9. Об утверждении Правил осуществления государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации: Постановление Правительства Российской Федерации (от 17.02.2018 г. № 162) [Электронный ресурс], информационно-правовой портал: http://www.garant.ru/products/ipo/prime/doc/71783452/ (Дата обращения: 20.11.2019).

10. Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования: Приказ ФСТЭК (от 21.12.2017 №235) [Электронный ресурс] : сайт Федеральной службы по техническому и экспортному контролю: https://fstec.ru/index?id=1606:prikaz-fstek-rossii-ot-21-dekabrya-2017-g-n-235 (Дата обращения: 20.11.2019).

11. Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации: Приказ ФСТЭК (от 25.12.2017 № 239) [Электронный ресурс] : сайт

Федеральной службы по техническому и экспортному контролю: https://fstec.ru/en/53-normotvorcheskaya/akty/prikazy/1592-prikaz-fstek-rossii-ot-25-dekabrya-2017-g-n-239 (Дата обращения: 20.11.2019).

12. Об утверждении формы акта проверки, составляемого по итогам проведения государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации: Приказ ФСТЭК России (от 11.12.2017 № 229) [Электронный ресурс]: сайт Федеральной службы по техническому и экспортному контролю: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/1475-prikaz-fstek-rossii-ot-11-dekabrya-2017-g-n-229 (Дата обращения: 20.11.2019).

13. Об утверждении формы направления сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий: Приказ ФСТЭК России (от 22.12.2017 № 236) [Электронный ресурс] : сайт Федеральной службы по техническому и экспортному контролю: https://fstec.ru/index?id=1607:prikaz-fstek-rossii-ot-22-dekabrya-2017-g-n-236 (Дата обращения: 20.11.2019).

14. О персональных данных: Федеральный Закон (от 27 июля 2006 г. №152-ФЗ) [Электронный ресурс] : справочная правовая система: http://www.consultant.ru/document/Cons_doc_LAW_61801/ (Дата обращения: 20.11.2019).

Научная и методическая литература

15. Безкоровайный Д. Безопасность компонентов / Д. Безкоровайный. – Открытые системы. СУБД. – М: Издательство «Открытые системы», 2011. – 26 с.

16. Бойченко О. В. Обеспечение безопасности критически важных объектов инфраструктуры российской федерации / А. А. Аношкина // Ученые записки Крымского федерального университета имени В. И. Вернадского. Экономика и управление, 2016 – С.15-19.

17. Жидко Е.А. Информационные риски как аргумент безопасного и

устойчивого развития организаций / Е.А. Жидко, Л.Г. Попова // Информация и безопасность, 2010. – №4. – С. 543–552.

18. Козин И.С. Метод определения опасности угрозы персональным данным при их обработке в информационной системе. 2017. – С. 19-26.

19. Кудрявцев А.М. Киберустойчивость информационно-телекоммуникационной сети / М.А. Коцыняк, И.А. Кулешов, А.М. Кудрявцев, О.С. Лаутаи. – СПб.: Бостон-спектр, 2015. – 150 с.

20. Куликов С.С. Метод риск–анализа информационно–телекоммуникационных систем при атаках на их ресурсы / С.С. Куликов, В.И. Белоножкин // Информация и безопасность, 2013. – Т. 16. – №1. – С. 143–144.

21. Меликов У.А. Гражданско-правовая защита персональных данных / У.А. Меликов // Вестник УрФО. Безопасность в информационной сфере. 2015. № 4 (18). – С. 49-53.

22. Михалевич И.В. Вопросы классификации объектов критической информационной инфраструктуры по требованиям безопасности информации / И.В. Михалевич // XIII Всероссийское совещание по проблемам управления, 2019 – С. 2587 – 2590.

23. Сидоренко В.Л. Защита объектов критической инфраструктуры в условиях гибридной технологии ведения войны / С.И. Азаров, Е.А. Власенко, В.А. Тищенко, 2018. – 14 с.

24. Соловьев В.В. Улучшение защищенности распределенной информационной системы персональных данных на основе технологии VPN и терминального доступа / В.В. Соловьев // Информационные технологии и проблемы математического моделирования сложных систем. – 2017. – №18. – С. 39-44.

25. Чукарин А.В. Бизнес-процессы и информационные технологии в управлении современной инфокоммуникационной компанией / А.В. Чукарин. – М.: Альпина Паблишер. – 2016. - 512 с.

Электронные ресурсы

26. Базовая модель угроз безопасности персональных данных при их

обработке в информационных системах персональных данных (Утверждена Заместителем директора ФСТЭК России 15 февраля 2008 г.) [Электронный ресурс] : сайт Федеральной службы по техническому и экспортному контролю: https://fstec.ru/component/attachments/download/289 (Дата обращения: 20.11.2019).

27. Банк данных угроз безопасности информации [Электронный ресурс] : сайт Федеральной службы по техническому и экспортному контролю: http://bdu.fstec.ru/ (Дата обращения: 20.11.2019).

28. Методика определения угроз безопасности информации в информационных системах персональных данных. ФСТЭК России, 2008 г. [Электронный ресурс] : сайт Федеральной службы по техническому и экспортному контролю: https://fstec.ru/component/attachments/download/290 (Дата обращения: 20.11.2019).

29. Фролов Я.О. Методы и средства обеспечения информационной безопасности на критически важных объектах народного хозяйства // XLIII междунар. студ. конф. № 8(43) [Электронный ресурс] : сайт научного издательства «СибАК»: https://sibac.info/archive/meghdis/8(43).pdf (Дата обращения: 20.11.2019).

Литература на иностранном языке

30. Arie H. Japan’s Approach to Tackling Cybersecurity Challenges, 2017 [Электронный ресурс] : новостной сайт: www.japanindustrynews.com/2017/01/japans-approach-tackling-cybersecurity-challenges/ (Дата обращения: 20.11.2019).

31. Bekeschenko E. Security of Critical Information Infrastructure: Legal Issues, 2017. [Электронный ресурс], Режим доступа: https://www.international-bc-online.org/wp-content/uploads/2017/09/5.-Bekeschenko-ENG.pdf (Дата обращения: 20.11.2019).

32. Giacomello G. Cybersecurity and critical information infrastructures, 2013 [Электронный ресурс] : сайт ISPI: https://www.ispionline.it/sites/default/files/pubblicazioni/analysis_201_2013.pdf

(Дата обращения: 20.11.2019)

33. Physical Protection of Critical Infrastructure against Terrorist Attacks, Trends Report, Counter Terrorism Executive Directorate, 2017 [Электронный ресурс]: сайт ООН: https://www.un.org/sc/ctc/wp-content/uploads/2017/03/CTED-Trends-Report-8-March-2017-Final.pdf (Дата обращения: 20.11.2019).

34. Shostack A. "Threat Modeling: Designing for Security", 2014 [Электронный ресурс] : сайт электронной библиотеки: https://avidreaders.ru/book/threat-modeling-designing-for-security.html (Дата обращения: 20.11.2019).

Приложение А

Порядок выявления и присвоения категорий объектам критической информационной инфраструктуры

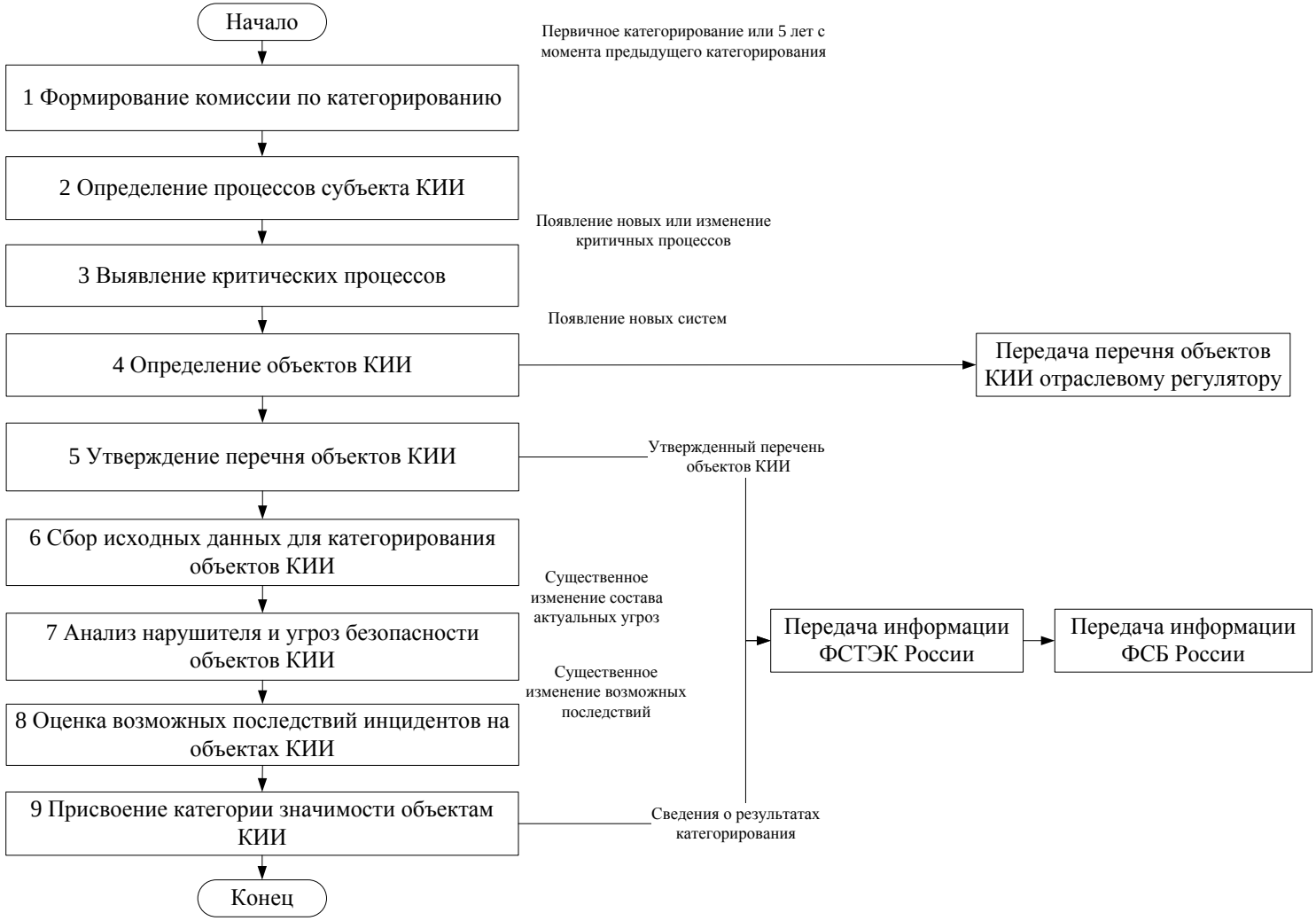

Рисунок А1 – Порядок выявления и присвоения категорий объектам критической информационной инфраструктуры

Приложение Б

Схема первого этажа медицинской организации

Рисунок Б1 – Схема 1-ого этажа медицинской организации ООО «Семейная поликлиника»

Рисунок Б2 – Схема 2-ого этажа медицинской организации ООО «Семейная поликлиника»

Приложение В

Топология локальной сети первого этажа медицинской организации

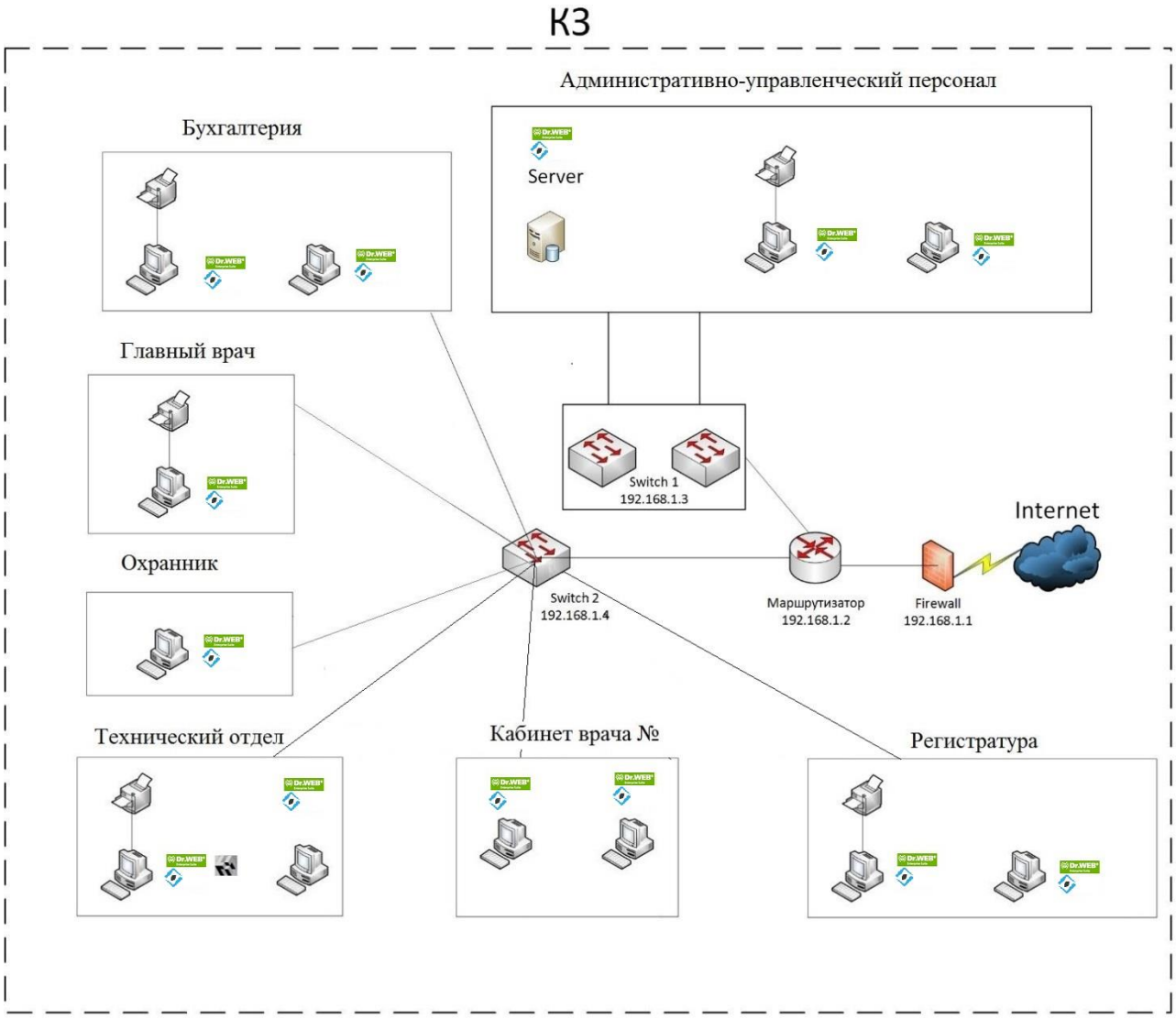

Рисунок В1 - Топология локальной сети 1-ого этажа медицинской организации ООО «Семейная поликлиника»

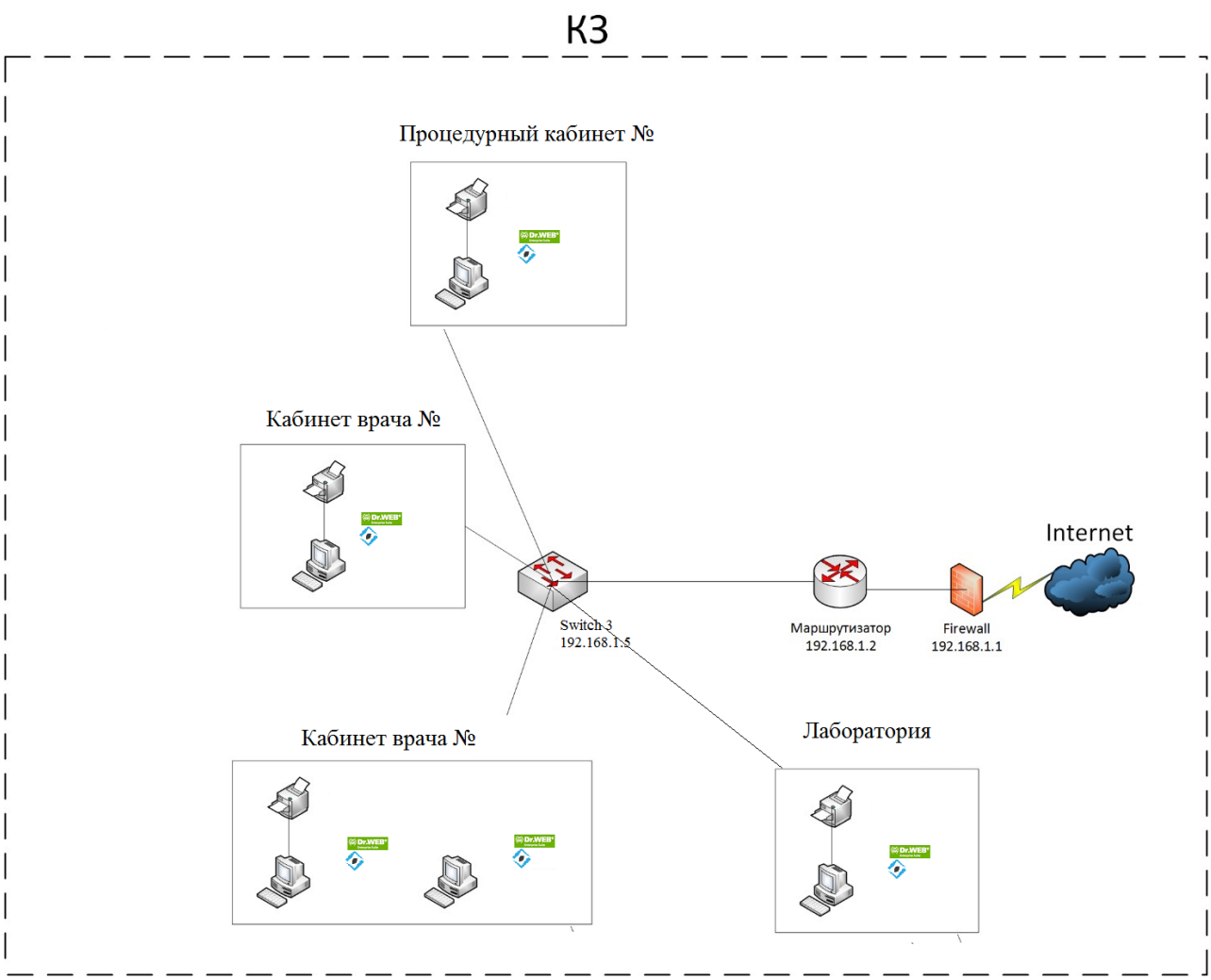

Рисунок В2 - Топология локальной сети 2-ого этажа медицинской организации ООО «Семейная поликлиника»

Приложение Г

Оценка актуальности угроз выявленных объектов критической информационной инфраструктуры организации

Таблица Г.1 – Оценка актуальности угроз выявленных объектов критической информационной инфраструктуры медицинской организации ООО «Семейная поликлиника»

Угроза безопасности объектов критической инфраструктуры ООО «Семейная поликлиника»	Источник угрозы безопасности	Потенциал нарушителя	Оценка возможности возникновения угрозы	Способ/Причина реализации
Угроза "Анализа сетевого трафика" с перехватом передаваемой по сети информации	Внешний нарушитель	Базовый	Неактуальная	Путем применения специальных средств и устройств
Угроза незаконного получения паролей и других реквизитов разграничения доступа с дальнейшим их использованием	Внутренний и внешний нарушитель	Базовый	Актуальная	Наличие санкционированного доступа в служебных целях
Угроза разглашения, передачи или утраты атрибутов разграничения доступа	Внутренний нарушитель	Базовый	Актуальная	В устной или письменной форме
Угроза удаленного запуска приложений	Внешний нарушитель	Базовый	Неактуальная	Путем применения специальных средств и устройств
Угроза перехвата конфиденциальной информации по сети	Внешний нарушитель	Базовый	Актуальная	Путем применения специальных средств и устройств
Угроза чтения остаточной информации из оперативной памяти и с внешних запоминающих устройств	Внутренний нарушитель	Базовый	Неактуальная	Путем применения специальных средств и устройств
Угроза чтения информации из областей оперативной памяти, используемых операционной системой	Внешний нарушитель	Базовый	Неактуальная	Путем применения специальных средств и устройств
Угроза несанкционированного использования терминалов пользователей, имеющих уникальные физические характеристики, такие как номер рабочей станции в сети, физический адрес, адрес в системе связи, аппаратный	Внутренний и внешний нарушитель	Базовый	Актуальная	Наличие санкционированного доступа в служебных целях

Продолжение таблицы Г.1

Угроза вскрытия криптографических шифров	Внутренний и внешний нарушитель	Базовый	Неактуальная	Путем применения специальных средств и устройств
Угроза реализации скрытого канала передачи данных	Внутренний нарушитель	Базовый усиленный	Актуальная	Наличие санкционированного доступа в служебных целях
Угроза незаконного подключение к линиям связи с целью прямой подмены законного пользователя, отключения после входа физическим путем с последующим вводом дезинформации	Внутренний и внешний нарушитель	Базовый	Неактуальная	Путем применения специальных средств и устройств
Угроза внедрения программных "закладок" и "вирусов"	Внутренний нарушитель	Базовый	Актуальная	Наличие санкционированного доступа в служебных целях
Угроза внедрения аппаратных закладок	Внутренний нарушитель	Базовый	Неактуальная	Наличие санкционированного доступа в служебных целях
Угроза применения подслушивающих устройств, дистанционная фото- и видеосъемка и т.п	Внутренний нарушитель	Базовый	Неактуальная	Наличие санкционированного доступа в служебных целях
Угроза внедрения агентов в число персонала системы	Внутренний нарушитель	Базовый	Актуальная	Взаимодействие с отделом кадров и лицом принимающим решение
Угроза вывода из строя подсистем обеспечения функционирования сети	Внутренний и внешний нарушитель	Базовый усиленный	Актуальная	Наличие санкционированного доступа в служебных целях и несанкционированного доступа
Кража, модификация, уничтожение информации	Внутренний и внешний нарушитель	Базовый	Актуальная	Путем применения специальных средств и устройств

Продолжение таблицы Г.1

Несанкционированное отключение средств защиты	Внутренний нарушитель	Базовый усиленный	Актуальная	Наличие санкционированного доступа в служебных целях
Угроза модификации системных файлов и средств защиты информации в целях вывод их из строя	Внутренний нарушитель	Базовый	Неактуальная	Наличие санкционированного доступа в служебных целях
Угрозы получения доступа к информации, основанные на использовании уязвимостей системного и прикладного ПО при нарушении условий эксплуатации как самого ПО, так и среды его функционирования	Внутренний и внешний нарушитель	Базовый	Неактуальная	Путем применения специальных средств и устройств
Установка ПО, не связанного с исполнением служебных обязанностей	Внутренний нарушитель	Базовый	Неактуальная	Наличие санкционированного доступа в служебных целях
Угроза неумышленного повреждения каналов связи	Внутренний нарушитель	Базовый	Неактуальная	В процессе исполнения служебных обязанностей
Непреднамеренная модификация (уничтожение) информации сотрудниками	Внутренний нарушитель	Базовый	Неактуальная	В процессе исполнения служебных обязанностей
Непреднамеренное отключение средств защиты	Внутренний нарушитель	Базовый	Неактуальная	В процессе исполнения служебных обязанностей
Сбой системы электроснабжения	Внутренний и внешний нарушитель	Базовый усиленный	Неактуальная	Наличие санкционированного доступа в служебных целях и несанкционированного доступа

Приложение Д

Оценка значимости объектов критической информационной инфраструктуры организации

Таблица Д.1 – Оценка значимости объектов критической информационной инфраструктуры ООО «Семейная поликлиника»

Показатель		Возможные значения показателя по ПП РФ № 127 от 08.02.2018			ИС, связанные с обслуживанием клиентов	ИС, связанные с обслуживанием сотрудников	АСУ пожаротушением	АСУ оборудованием	Корпоративная сеть
		III категория	II категория	I категория					
I.	Социальная значимость								
1	Причинение ущерба жизни и здоровью людей (человек)	более или равно 1, но менее или равно 50	более 50, но менее или равно 500	более 500	более или равно 1, но менее или равно 50	более или равно 1, но менее или равно 50	более или равно 1, но менее или равно 50	более или равно 1, но менее или равно 50	-
5	Отсутствие доступа к государственной услуге, оцениваемое в максимальном допустимом времени, в течение которого государственная услуга может быть недоступна для получателей такой услуги (часов)	менее или равно 24, но более 12	менее или равно 12, но более 6	менее 6	менее или равно 24, но более 12	менее или равно 24, но более 12	менее или равно 24, но более 12	менее или равно 24, но более 12	-
9	Возникновение ущерба бюджетам Российской Федерации, оцениваемого								
а)	В снижении доходов федерального бюджета, (процентов прогнозируемого годового дохода бюджета)	более 0,001, но менее или равно 0,05	более 0,005, но менее или равно 0,1	более 0,1	более 0,001, но менее или	более 0,001, но менее или	более 0,001, но менее или	более 0,001, но менее или	-

					равно 0,05	равно 0,05	равно 0,05	равно 0,05	

Продолжение Приложения Д

Таблица Д.1 – Оценка значимости объектов критической информационной инфраструктуры ООО «Семейная поликлиника»

б)	В снижении доходов бюджета субъекта Российской Федерации (процентов прогнозируемого годового дохода бюджета)	более 0,001, но менее или равно 0,05	более 0,05, но менее или равно 0,1	более 0,1	более 0,001, но менее или равно 0,05	более 0,001, но менее или равно 0,05	более 0,001, но менее или равно 0,05	более 0,001, но менее или равно 0,05	-
в)	В снижении доходов бюджетов государственных внебюджетных фондов (процентов прогнозируемого годового дохода бюджета)	более 0,01, но менее или равно 0,5	более 0,5, но менее или равно 1	более 1	более 0,01, но менее или равно 0,5	более 0,01, но менее или равно 0,5	более 0,01, но менее или равно 0,5	более 0,01, но менее или равно 0,5	-