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)
Технология бизнес-анализа
(направленность (профиль))

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА (МАГИСТЕРСКАЯ ДИССЕРТАЦИЯ)

на тему Исследование технологий обеспечения комплексной информационной безопасности в государственном учреждении

Обучающийся Р. Я. Склюев
(Инициалы Фамилия) (личная подпись)

Научный руководитель д-р. социол. наук, доцент Е. В. Желнина
(ученая степень (при наличии), ученое звание (при наличии), Инициалы Фамилия)

Тольятти 2023

Оглавление

Введение

Обоснование выбора темы магистерской диссертации и ее актуальности. Выбранная тема является очень актуальной в условиях современных организациях, что объясняется:

– постоянным ростом количества различных информационных угроз в виде вредоносного и вирусного программного обеспечения;

– динамикой развития и совершенствования основных подходов и принципов защиты данных, которая не в состоянии идти в ногу с динамикой развития современных информационных технологий;

– стремительным ростом объемов обрабатываемых данных, что влечет к увеличению ПК. Следствием этого является высокая активность злоумышленников, осуществляющих деятельность;

– низкая степень защищенности информации и данных вследствие ее доступа через различные корпоративные и мобильные сети связи;

– свободным доступом персональных компьютеров к глобальным базам данных привел к всеобщему распространению грамотности в информационной сфере среди широких слоев населения. Данный аспект способствует увеличению количества вирусных программ.

Научная новизна. Научная новизна исследования состоит в разработке и внедрении методических и методологических рекомендация по организации информационной безопасности государственных учреждений медицинской сферы и включает в себя: разработку модели информационной инфраструктуры государственных учреждений медицинской сферы; разработку модели информационной безопасности государственных учреждений медицинской сферы; разработку методов защиты информации в государственных учреждений медицинской сферы; разработке модели проектной защиты.

Постановка научной проблемы исследования. Очевидно, что на сегодняшний день поиск эффективных и современных средств защиты информации и баз данных представляет собой весьма актуальную задачу

в условиях современных организаций с наличием корпоративных сетей. Одним из таких средств является программно-аппаратное обеспечение. Однако, оно не в состоянии обеспечить требуемую безопасность без применения дополнительных средств защиты информации. В связи с уязвимостью информационных ресурсов большое количество организаций и предприятий несут значительные экономические потери.

Тема настоящей выпускной квалификационной работы – «Технологии обеспечения комплексной информационной безопасности в государственном учреждении». Работа выполнена на базе Государственного бюджетного учреждения «Курганская больница скорой медицинской помощи».

Специфика развития и текущего состояния информационных систем требует надежной, эффективной и комплексной системы информационной безопасности всех современных корпоративных систем. Данная проблема решается путем разработки и интеграции современных инструментов и комплексов, способных обеспечить комплексную систему защиты информационных баз. Деятельность злоумышленников все чаще направлена на хищение различных физических носителей информации, содержащих личные данные и прочую конфиденциальную информацию. Таким образом, очень востребованными являются современные и высокоэффективные технические средства и различные мероприятия организационного характера, которые способны обеспечить требуемый уровень безопасности личных данных и конфиденциальной информации [12].

Все современные организации и предприятия сталкиваются с проблемой обеспечения высокого уровня безопасности и защиты баз данных и информации. Также высокой актуальностью характеризуется и проблема обеспечения надежной защиты ресурсов корпоративных сетей предприятий и организаций. Подавляющее большинство современных организаций и предприятий не ограничиваются пределами какого-либо одного здания, что обусловлено распределенным характером их структуры.

Объект исследования – государственное бюджетное учреждение

больница скорой медицинской помощи выполняет критическую роль в обеспечении населения неотложной медицинской помощью в случаях, когда здоровье и жизни людей находятся под угрозой.

Вместе с ростом использования информационных технологий и электронных медицинских систем в больницах появляются новые вызовы и угрозы в области информационной безопасности. Защита конфиденциальности пациентов, предотвращение несанкционированного доступа к медицинской информации и обеспечение целостности данных становятся основными приоритетами.

Цель выпускной квалификационной работы – разработка методики обеспечения комплексной информационной безопасности медицинской организации.

Объект исследования – система комплексной информационной безопасности в учреждении здравоохранения.

Предмет исследования – методика обеспечения комплексной информационной безопасности медицинской организации.

Гипотеза исследования – применение современных методик комплексной информационной безопасности медицинской организации должно обеспечить заданный уровень ИБ данных объектов.

Исходя из цели выпускной квалификационной работы, в процессе ее выполнения необходимо решить следующие задачи:

– исследовать основные понятия информационной безопасности и особенности ее обеспечения в медицинских организациях;

– произвести анализ нормативно-правового обеспечения информационной безопасности медицинских организаций;

– произвести анализ методов внутреннего аудита информационной безопасности медицинских организаций и постановка задачи ВКР;

– разработать типовую модель угроз информационной безопасности медицинской организации;

– разработать типовую модель нарушителя информационной

безопасности медицинской организации;

– произвести анализ функциональных возможностей системы программно-аппаратных средств защиты медицинской организации для проведения внутреннего аудита информационной безопасности;

– разработать основные процедуры методики обеспечения комплексной информационной безопасности медицинской организации с применением системы программно-аппаратных средств защиты;

– произвести оценку эффективности разработанных решений.

Определение теоретических основ исследования. Работа базируется на научных трудах отечественных и зарубежных авторов, таких как А. П. Трубачев, М. Ю. Долинин, М. Т. Кобзарь, А. А. Сидак, Е. Б. Белов, В. П. Лось, Р. В. Мещеряков, А. А. Шелупанов, Д. М. Ахмад, И. Дубравский и других.

Методологический аппарат исследования. Выпускная квалификационная работа основывается на таких методах, как: комплексный анализ теоретических основ и имеющейся литературы по рассматриваемой тематике, анализ действующих законодательных и нормативных актов, а также анализ имеющихся исследований по теме обеспечения информационной безопасности в условиях современных организаций и предприятий. Основными теоретическими методами исследования при написании данной магистерской диссертации являются исследование рассматриваемого объекта проектирования и анализ современных средств и комплексов защиты данных, которые в наибольшей степени подходят к конкретным условиям. Среди практических методов исследования необходимо отметить: методика сравнения, анализа и исследования с целью объективного представления текущего состояния на рассматриваемом объекте.

Теоретическая и практическая значимость – результатом работы будут являться рекомендации по внедрению решений в области программно-аппаратных средств защиты, что повысит уровень информационной безопасности исследуемого учреждения.

Выпускная квалификационная работа обладает большой теоретической

значимостью, так как при ее написании будет изучен большой объем теоретических данных, которые являются необходимым атрибутом при трудовой деятельности в сфере информационной безопасности.

Высокая степень защищенности и безопасности информационных ресурсов представляет собой одну из важнейших задач, которые стоят как перед отдельными организациями и предприятиями, так и перед государством в целом. Для решения этой задачи необходимо обеспечить высокий уровень безопасности информационных ресурсов на предприятиях и организациях всех масштабов, начиная от мелких частных контор и заканчивая государственными бюджетными структурами, которые являются системообразующими.

Положения, выносимые на защиту магистерской диссертации «Исследование технологий обеспечения комплексной информационной безопасности в государственном бюджетном учреждении «Курганская больница скорой медицинской помощи»:

1. Основными угрозами информационной безопасности в государственном учреждении являются несанкционированный доступ к медицинской информации, утечка персональных данных сотрудников и пациентов, нарушение целостности, конфиденциальности и доступности системы, а также риск кибератак со стороны злоумышленников.

2. Определены ключевые меры по обеспечению информационной безопасности в государственном учреждении, включающие в себя: разработку политики информационной безопасности, регулярное обновление и обучение персонала, установку современных технических средств защиты, создание резервных копий данных и восстановление после инцидентов, а также мониторинг и анализ уязвимостей системы.

3. Проведено исследование эффективности внедрения выбранных технологий обеспечения информационной безопасности в государственном учреждении. Результаты показали, что использование данных технологий значительно снижает риск инцидентов информационной безопасности.

4. В результате внедрения технологий обеспечения комплексной информационной безопасности в государственном учреждении достигнуты следующие положительные результаты:

– снижение уровня угроз и рисков, связанных с несанкционированным доступом к медицинской информации и утечкой персональных данных пациентов;

– обеспечение целостности и доступности информационных систем, что способствует бесперебойному предоставлению медицинской помощи и улучшению качества услуг;

– улучшение реагирования на кибератаки и обнаружение инцидентов, благодаря системам мониторинга и обнаружения инцидентов;

– повышение уровня осведомленности и компетенции персонала в области информационной безопасности;

– создание эффективной системы управления доступом и аутентификации, обеспечивающей контроль и защиту информации.

Применение современных технологий и методов позволяет снизить риски и угрозы, связанные с информационной безопасностью, обеспечивает защиту медицинской информации и персональных данных пациентов, а также гарантирует бесперебойное функционирование системы и предоставление качественной медицинской помощи. Это исследование и внедрение технологий обеспечения комплексной информационной безопасности в государственном учреждении имеет практическую значимость и может быть использовано в других организациях здравоохранения для повышения уровня защиты и безопасности информации. Результаты и рекомендации, представленные в данной магистерской диссертации, могут быть использованы администрацией и специалистами в области информационной безопасности для принятия обоснованных решений и внедрения эффективных мер по защите информации.

Общий вывод состоит в том, что разработка и применение технологий обеспечения комплексной информационной безопасности является важным

фактором для успешного функционирования и защиты государственных учреждений здравоохранения. Это позволяет обеспечить конфиденциальность, целостность и доступность медицинской информации, а также снизить риски и угрозы, связанные с несанкционированным доступом и утечкой данных.

Объем и структура диссертации. Работа включает в своем составе введение, три главы основной части, заключение, список использованных источников, приложения. Объем работы – 105 страниц, в том числе 10 иллюстраций, 16 таблиц и 2 приложения.

Глава 1 Анализ теоретических и правовых аспектов обеспечения информационной безопасности медицинских организаций

1.1 Анализ литературных источников по теме исследования

Существует большое количество научных статей и книг по рассматриваемой в данной работе теме. Широкое освещение вопросов современных информационных систем обусловлено их эффективностью и повсеместным использованием в условиях медицинских организаций, а также объектов здравоохранения. В настоящей главе будет проведен анализ наиболее известных и распространенных литературных источников, которые освещают вопросы использования информационных систем для автоматизации процессов в условиях медицинским учреждений [1].

Научное издание под названием «Основы проектирования информационных систем и технологий», авторами которого являются В. В. Бова и Ю. А. Кравченко [7], содержит много информации об основах и принципах эффективного проектирования информационных систем и программных продуктов для автоматизации обработки информации.

Еще одним популярны и известным литературным изданием по рассматриваемой тематике является книга под названием «Проектирование информационных систем» [8]. Эта книга написана коллективом авторов во главе с В. М. Вейцманам Книга охватывает широкий спектр вопросов, среди которых: степень необходимости и эффективности финансирования таких областей развития предприятия или организации как автоматизация обработки информационных ресурсов и баз данных, формирования планов развития информационной составляющей, создание высокоэффективных информационных проектов и т. д. За счет использования авторами современных методик анализа и прогнозирования в сфере информационных технологий, ими создан алгоритм определения степени актуальности и целесообразности проведения модернизации имеющихся информационных

систем. Еще одна из предлагаемых методик в данной книге позволяет определить наиболее эффективный способ повышения производительности. В отельной главе авторы дают подробный анализ современных наиболее эффективных и используемых систем управления информационными ресурсами в условиях организаций здравоохранения.

Научный труд под названием «Информационные технологии», авторами которого являются Г. С. Гохберг, А. В. Зафиевский и А. А. Короткин. [14], посвящен вопросам изучения необходимого уровня квалификации и определения спектра задач, которые необходимо решать силами специалистов по созданию и отладке современных информационных систем в сферах здравоохранения и медицинских учреждений. Для того, чтобы успешно и эффективно решать поставленные задачи необходимо выполнение целого ряда операций, а именно: тщательный анализ и изучение объекта, для которого планируется создание информационной системы, создание перечня требований, которые предъявляются к разрабатываемой системе, определение перечня тех инструментов программирования, которые в наибольшей степени способны решить поставленные перед ними задачи. При написании данной книги коллектив авторов использовал в качестве теоретической основы опыт зарубежных и отечественных специалистов в сфере автоматизации и информационных систем. Вся содержащаяся информация в книге основана как на отечественном, так и на зарубежном опыте в сфере разработки и эксплуатации информационных систем. Основными методиками, которые предлагаются авторами книги для проектирования и создания ИС являются: функциональный анализ, теоретическое и практическое исследование, и т. д. Системность и полнота данной книги обусловили ее широкое применение в качестве базы для создания различных обучающих программ и курсов по изучению основ создания информационных систем. Также данная книга содержит в своем составе практический пример проектирования и реализации информационной системы на примере

реальной организации. За счет наличия практических примеров обучаемые могут на реальном примере проследить процесс формирования требований и проектирования ИС.

В процессе эволюции и развития систем автоматизации информационного взаимодействия было установлено, что организационная составляющая абсолютно всех информационных систем является наиболее важной среди всех остальных подсистем. К этому выводу практически одновременно пришли и отечественные и зарубежные специалисты в данной отрасли. Как правило, степень эффективности функционирования практически всех предприятий и организаций, в первую очередь, зависит от наличия в их структуре эффективных и высокопроизводительных информационных систем с помощью которых можно автоматизировать большинство операций документооборота и составления различных отчетов по результатам деятельности [2].

В настоящее время среди большого количества различных секторов экономики и бизнеса наиболее динамично развиваются именно те, которые осуществляют свою деятельность в сфере информационных систем. Эта тенденция справедлива не только для зарубежных организаций, но и для отечественных предприятий. При изучении спроса на программные продукты и информационные системы можно прийти к выводу, что наибольшим спросом они пользуются именно у организаций и предприятий государственного сектора. Таким образом, очевидно, что высокий уровень спроса носит устойчивый и стабильный характер в течение большого промежутка времени вне зависимости от экономической обстановки и прочих факторов [11].

Перед разработчиками современных информационных систем стоит целый ряд довольно сложных задач, что объясняется необходимостью решения обширного перечня задач с помощью ИС. Наиболее важными и значительными задачами, которые стоят перед современными информационными системами, являются: высокая эффективность

организации документооборота, формирование базы данных с необходимым перечнем нормативно-правовой документации, систематизация всех информационных ресурсов организации.

1.2 Основные понятия информационной безопасности и особенности ее обеспечения в медицинских организациях

В настоящее время основным направлением в сфере развития информационных технологий является создание эффективной системы безопасности информационных и компьютерных систем [13].

Под термином информационная защита подразумевается комплекс мероприятий, который направлен на обеспечение необходимого уровня защиты баз данных от негативного действия вредоносного программного обеспечения, а также защиту информации от несанкционированного доступа третьих лиц.

Объектом защиты является непосредственно информация, которая может храниться на каком-либо носителе и быть доступной определенной группе пользователей. Относительно этой информации осуществляется комплекс мероприятий по ее защите от доступа злоумышленников и кражи.

Основная преследуемая цель заключается в обеспечении высокого уровня защиты данных. В процессе реализации системы безопасности информационных ресурсов обеспечивается ее надежная защита от различных угроз в виде хищения, порчи, изменения и утечки, которые могут стать причиной значительных финансовых потерь.

Под термином эффективности системы информационной безопасности подразумевается соответствие целей и результатов при организации системы безопасности информационных ресурсов.

Для того, чтобы обеспечить должный уровень информационной защиты необходимо решить комплекс задач относительно обеспечения таких требований, как конфиденциальность, целостность и достоверность

информационных ресурсов, которые подлежат хранению, обработке и передаче.

Под термином информационная защита подразумевается комплекс мероприятий, который направлен на обеспечение необходимого уровня защиты баз данных от негативного действия вредоносного программного обеспечения, а также защиту информации от несанкционированного доступа третьих лиц [4]. Наличие правильной политики организационной безопасности важно в контексте развития организации в любой сфере, включая и государственный сектор. Понимание важности требований стандартов международного уровняв сфере защиты информации позволяет компании из государственного сектора вести стабильную и прогнозируемую деятельность. Чтобы добиться безопасности в отношении собственных данных, организации в данной сфере важно создать собственные процессы управления информацией, базами данных и технологиями и впоследствии поддерживать их работоспособность на высоком уровне. Не менее важно добиться такого состояния, когда будет наблюдаться доступность и целостность создаваемой и передаваемой информации [28].

Требования в сфере информационной безопасности следует принимать в расчет при создании новых информационных систем и методов управления. Еще один важный момент касается необходимости соответствия масштабу применения СМИБ и потребностей государственной компании. СМИБ государственной организации может использоваться также третьими лицами, включая и возможность закрывать те требования, что устанавливает ИБ.

Благодаря созданию комплексной политики ИБ для государственной компании можно выполнить следующие задачи:

– создать свою систему безопасности информации для государственной организации;

– анализ СМИБ, которая применяется для защиты данных, и

напрямую связано с финансовой деятельностью компании;

– оценить СМИБ организации в контексте сохранения данных по сотрудникам и защиты интеллектуальной собственности;

– оптимизировать данные в рамках СМИБ, которые доверяют государственному учреждению другие компании.

Процесс обеспечения комплексной безопасности информации государственной компании, которое включает в себя следующие аспекты:

– устранение возможности проникновения к информационным ресурсам государственной компании со стороны злоумышленников;

– применение сотрудниками организации таких систем и элементов, которые не позволяют беспрепятственно распространять персональные данные;

– разделение прав доступа пользователей для применения данных;

– создание такой ситуации, когда потеря, утечка и блокировка важных данных со становится невозможной;

– создание баз информации для достижения наибольшей ее достоверности, сохранности и целостности

Подчас государственные учреждения создают специализированные отделы для того, чтобы предотвратить возможность получения злоумышленниками важной информации, в том числе и персональных данных. Специалисты подобных подразделений должны решать различные вопросы, в том числе и безопасное хранение данных, создание и применение средств защиты данных, разделение прав доступа к данным, применение сложных паролей для доступа к данным [28].

Комплексное соответствие СМИБ для государственного учреждения на предмет существующих требований происходит при соблюдении норм существующей документации стандартов. Так, в сфере СМИБ действует ряд стандартов, которые созданы под структурой ISO и IEC. Указанные стандарты действуют в сфере «Информационные технологии. Методы обеспечения безопасности», при этом каждый документ имеет свою область

использования и затрагивает тот или иной аспект ИБ [28].

В настоящее время практически вся информация обрабатывается с использованием средств вычислительной техники. Все компьютеры и серверы, как правило, объединяются в локальные компьютерные сети. Локальные компьютерные сети, в свою очередь, могут иметь доступ в сеть Интернет. В связи с этим наибольшая угроза безопасности информационным ресурсам исходит именно из сети Интернет. В подавляющем большинстве случаев объектом хакерских атак являются не сами данные и их носители, а программное обеспечение, которое осуществляет работу с данными. Помимо этого, довольно широко распространены атаки на ПО, которое является сервисным и также осуществляет работу с информационными ресурсами и носителями данных. Как правило, большинство программ предназначены для работы с информационными ресурсами, которые относятся к классу прикладных данных. Для систематизации хранящейся информации она объединяется в информационные системы на основе определенных признаков и критериев. Информационные системы наиболее часто подвержены атакам со стороны вредоносного ПО и злоумышленников.

К угрозам информационной безопасности относят:

– нарушение конфиденциальности (утечка, разглашение);
– нарушение работоспособности (дезорганизация работы);
– нарушение целостности и достоверности информации.

Рассмотрим основные, наиболее важные понятия, касающиеся тематики информационной безопасности.

Основное направление развития информационных технологий направлено на обеспечение информационной безопасности компьютерных систем и программно-аппаратных средств [5].

В современных условиях информация является базовой основой в процессе деятельности как отдельного человека, так и общества в целом. Вместе с развитием науки происходит неизбежное усложнение

информационной модели мира. Качество жизни человечества напрямую зависит от степени понимания протекания информационных процессов [7].

Ввиду активной цифровизации и с ростом рисков по утечке и мошенническом использовании информации вопрос о персональных данных стоит крайне остро. При проведении проверок инспекторы особое внимание обращают на документы, относящиеся к персональным данным, их наличие, хранение, согласие работников на обработку и т. д.

Обобщенно классификацию методов защиты информации можно представить в виде схемы, представленной на рисунке 1.

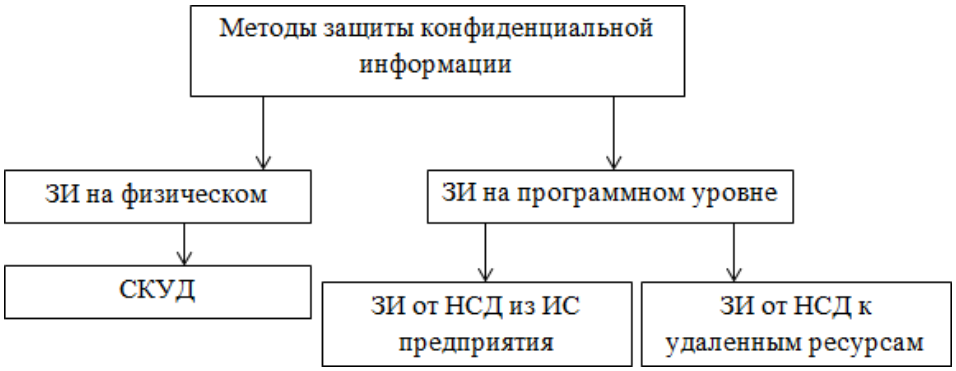

Рисунок 1 – Общая классификация методов защиты информации

Рассмотренная выше классификация средств обеспечения безопасности является всеобъемлющей и в общем случае может быть рекомендована для внедрения в государственных учреждениях или частных компаниях [49].

1.3 Анализ нормативно-правового обеспечения информационной безопасности медицинских организаций

В Российской Федерации в области обеспечения ИБ действует ряд законов. Для большего понимания нормативно-правовой базы по исследуемой тематике следует рассмотреть наиболее значимые

законодательные акты по данной тематике [30].

Вступивший в силу Приказ № 21 [8] от 18 февраля 2013 года, определяет и уточняет организационные и технические меры по защите персональных данных. Он многократно дополнялся и менялся, опираясь на развитие технологий. В последней редакции от 2017 года содержатся рекомендации, регулирующие:

– идентификацию и аутентификацию лиц, которых операторы допускают к обработке персональных данных;

– управление системой доступа к ним;

– программную среду и ее ограничения;

– защиту компьютеров, которые содержат информацию, относящуюся к персональным данным;

– порядок регистрации инцидентов безопасности;

– способы фиксации проникновения в защищенный информационный периметр;

– порядок организации антивирусной защиты;

– контроль защищенности персональных данных;

– защиту технических средств.

На смену ФЗ № 24-ФЗ ФЗ «Об информации, информационных технологиях и о защите информации», регламентирующий следующие аспекты:

– доступ лиц к работе с информационными ресурсами, которые представляют собой закрытую конфиденциальную информацию;

– правила обменом информацией, которая является потенциальным объектом атаки со стороны злоумышленников;

– основные принципы построения высокоэффективных систем защиты информации.

В рассматриваемом нормативно-правовом документе нет информации о правилах пользования и обмена информации, которая представляет собой интеллектуальную собственность.

Основное назначение этого закона состоит в четком распределении прав и обязанностей лиц, работающих с информацией, которая является потенциальным объектом атаки со стороны злоумышленников.

Помимо законов на начальных этапах деятельности по созданию и модернизации законодательства в области защиты информации изданы соответствующие указы Президента РФ.

В РФ действует утвержденная Президентом Доктрина информационной безопасности. В основе этого документа лежит комплекс целей, принципов, а также основных направлений в сфере обеспечения информационной безопасности РФ. В основе доктрины информационной безопасности лежат следующие принципы:

- под информационной безопасностью следует понимать такую степень защищенности информационных ресурсов той или иной базы данных, при которой соблюдается баланс интересов как государства в целом, так и его граждан в частности;
- в сфере информационной безопасности основными и наиболее опасными являются преступления, направленные на подрыв и нарушение конституционных прав граждан, а также на нарушение прав в сфере информационной деятельности [26].

1.4 Анализ методов внутреннего аудита информационной безопасности медицинских организаций и постановка задачи обеспечения комплексной информационной безопасности

Угроза безопасности информационной системы является актуальной если ее относительно легко реализовать на практике в отношении реальной информационной системы. Определение списка актуальных угроз безопасности информационной системы рассматриваемой организации осуществляется в соответствии с рассмотренной ранее методикой [4]. Произведем сравнение методов внутреннего аудита ИБ – таблица 1.

Таблица 1 – Сравнение методов внутреннего аудита ИБ

Критерии	Вид аудита		
	Активный	Экспертный	На соответствие стандартам
Угрозы	Высокая стоимость необходимого программного обеспечения Для каждой системы необходимо выбрать программное обеспечение для проведения аудита Возможны ошибки в используемом программном обеспечении	Отсутствие автоматизации процесса. Необходимость доверять экспертом. Высокие требования к компетентности экспертов. Есть противоречия во мнениях экспертов.	Большое количество юридических документов Нормативно- правовая база постоянно совершенствуется. Противоречия в юридических документах. Невозможно выполнить аудиторские полномочия силами самой организации.
Возможности	Высокий спрос на рынке. Аудит может осуществляться сотрудниками подразделения информационной безопасности предприятия. Автоматизировать большую часть работы экспертов.	Наличие необходимых юридических документов. Проверка может быть выполнена сотрудниками предприятия подразделений информационной безопасности Возможность автоматизировать процесс аудита	Сертификат безопасности выдается в результате аудита для улучшения имиджа компании. В требованиях нормативных документов находят отражение лучшие практические выводы экспертов Высокий спрос на рынке
Сильные стороны	Автоматизация процесса аудита. В ходе проведения аудита не требуется участия сотрудников компании. Возможно проведение стресс- тестирования для определения производительности и устойчивости системы.	Никакого дополнительного ПО. На время проведения ревизии не нужно останавливать работу системы Ревизия исходит из угроз информационной безопасности	Порядок проведения аудита регламентируется нормативными актами, в которых присутствует описание отчетных документов. Никакого дополнительного ПО Не требуется прекращение работы системы в ходе проведения аудита.

Для того, чтобы определить вероятность практической реализации потенциальной угрозы необходимо оценить два параметра: степень защиты

информационной системы, а также вероятная частота ее возникновения. Первый параметр представляет собой показатель, величина которого определятся как эксплуатационными, так и техническими особенностями информационной системы. Эти особенности перечислены в таблице, которая содержится в методических рекомендациях по созданию модели угроз ИБ [4].

Произведем анализ уязвимостей объекта защиты информации – типового учреждения здравоохранения.

Для типового учреждения здравоохранения выявлены ниже представленные информационные активы.

Информационный актив № 1: документы, имеющие отношение к планам развития учреждения здравоохранения и содержащие следующую информацию:

– информация о планах развития учреждения здравоохранения;

– документация о сделках с подрядчиками;

– медицинские программы.

Информационный актив № 2: документы, имеющие отношение к непосредственной деятельности учреждения здравоохранения:

– персональные данные пациентов и сотрудников;

– бюджеты, финансовая информация;

– отчеты о работе структурных подразделений.

Физический актив № 1: резервные копии информационной системы учреждения здравоохранения.

Результаты оценки уязвимости активов учреждения здравоохранения приведены в таблице 2.

Таблица 2 – Результаты оценки уязвимости активов учреждения здравоохранения

Группа уязвимостей Содержание уязвимости	Информационный актив № 1	Информационный актив № 2	Физический актив № 1
Среда и инфраструктура			
Незащищенное хранение.			низкая
Отсутствие или некорректная политика контроля доступа.			средняя
Аппаратное обеспечение			
Подверженность влажности, пыли и загрязнению.			низкая
Подверженность перепадам температур.			низкая
Подверженность колебаниям напряжения.			низкая
Контроль доступа			
Неправильное разграничение доступа в сетях.	средняя	средняя	
Отсутствие защиты мобильного компьютерного оборудования.	низкая	низкая	
Плохое управление паролями (хранение пароля, легко угадываемые пароли и т. д.).	средняя	средняя	
Коммуникации			
Незащищенное соединение с сетями общего пользования.	средняя	средняя	
Отсутствие обновления операционных систем и программного обеспечения.	низкая	низкая	
Неконтролируемое копирование.	высокая	высокая	
Отсутствие процедур резервного копирования.	высокая	высокая	
Персонал			
Неосведомленность в вопросах безопасности	низкая	низкая	низкая
Не отменяются права доступа после увольнения	средняя	средняя	
Общие уязвимые места			
Неконтролируемая загрузки и использование программного обеспечения.	средняя	средняя	

Результаты оценки рисков угроз безопасности персональных данных информационных систем медицинского учреждения приведены в таблице 3.

Таблица 3 – Результаты оценки рисков угроз безопасности персональных данных информационных систем медицинского учреждения

Группа угроз Содержание угроз	Информационный актив № 1	Информационный актив № 2	Физический актив № 1
Угрозы, обусловленные преднамеренными действиями			
Кража компьютерного оборудования и носителей информации.			низкая
Утечка конфиденциальной информации из сети по каналам связи	средняя	средняя	
Перехват информации на линиях связи путем использования различных видов анализаторов сетевого трафика.	низкая	низкая	
Угрозы, обусловленные случайными действиями			
Утечка конфиденциальной информации в следствии утери мобильных устройств	низкая	низкая	
Разрушение данных по причине системного сбоя или ошибки ПО	низкая	низкая	
Угрозы, обусловленные естественными причинами (природные, техногенные факторы)			
Затопление, пожар, ураган, землетрясение и т. п.	низкая	низкая	низкая

После того, как был проведен анализ всех потенциально вероятных угроз безопасности информационных ресурсов организации было установлено, что наиболее ожидаемой угрозой является несанкционированный доступ злоумышленников к закрытой информации из базы данных рассматриваемой организации. На следующем этапе исследования требуется более детально провести анализ именно этой угрозы.

При проведении аудита возможно использование нескольких стратегий – таблица 4.

Таблица 4 – Стратегии проведения аудита ИБ

Учитываемые угрозы при проведении аудита ИБ	Влияние на информационные системы		
	отсутствует	частичное	существенное
Наиболее опасные	Оборонительная стратегия		
Все идентифицированные угрозы		Наступательная стратегия	
Все потенциально возможные			Упреждающая стратегия

Упреждающая методики предполагает исследование всех возможных угроз для системы и разработку мер по их упреждению уже на стадии проектирования системы. Неотъемлемой частью данной методики является анализ информации центров изучения проблем информационной безопасности [13].

Для проведения работ по исследованию эффективности системы безопасности информационных ресурсов между заказчиком и исполнителем работ заключается соответствующий договор. В этом договоре уточняются все условия сотрудничества, а именно: цели и сроки проведения проверки, способы проведения проверки и т. д.

Как правило, работ по исследованию эффективности системы безопасности информационных ресурсов заключаются в проведении следующих мероприятий:

– Составление перечня основных целей и задач, которые необходимо решить в процессе проведения работ.

– Со стороны заказчика работ исходит информация об объектах проведения проверки эффективности системы безопасности информационных ресурсов. Как правило, при проведении комплексной проверки всех ресурсов сети достигается максимальная эффективность. Вместе с этим стоимость такого объема работ может оказаться очень высокой и неприемлемой для заказчика. С целью оптимизации расходов на проведение проверок, исполнителем работ предлагается ограничить круг

исследуемых объектов. При типовой организации нескольких сетей в организации, уровень их безопасности может быть исследован на примере одной из этих сетей. В этом случае эффективно выявляются типовые недостатки и уязвимые места сети, которые характерны для всей группы однотипных ЛВС. Таким образом, при проведении исследования остальных сетей уже заранее известны некоторые уязвимые ее части.

– Получение доступа ко всем ресурсам сети, которые необходимы для проведения работ по исследованию эффективности ее защиты.

На этом этапе исполнитель работ осуществляет сбор всей необходимой информации об информационных потоках внутри исследуемой сети. При этом учитываются и внешний информационные потоки. Также проводится работа по исследованию всего имеющегося и применяемого оборудования – ЭВМ, серверное оборудование, периферийные устройства и т. д. [25].

– Анализ и исследование всех информационных потоков в рассматриваемой сети.

При этом осуществляется проверка уровня безопасности всех рабочих мест организации. В процессе анализа и исследования всех информационных потоков в рассматриваемой сети проводятся следующие мероприятия:

– анализ соблюдения требований и правил информационного взаимодействия персонала;

– анализ уровня знаний рабочего персонала основных правил безопасного информационного обмена данными;

– оценка эффективности имеющихся регламентов по информационной безопасности;

– проверка эффективности имеющейся системы защиты информации;

– проверка эффективности работы программного обеспечения по защите от вирусов;

– изучение всех случаев попыток взлома и хищения информации;

– анализ эффективности используемых средств программного и аппаратного противодействия утечкам информации;

– анализ степени безопасности информации при применении периферийных запоминающих устройств при обмене информацией;

– анализ уровня безопасности при работе сотрудников организации во внешней сети Интернет;

– анализ уровня безопасности информационных ресурсов при работе с ними лиц, не являющихся сотрудниками рассматриваемой организации;

– анализ уровня защиты сетей организации от попыток незаконного доступа к хранящейся информации.

Проведение мероприятий по комплексной проверке устройств, с помощью которых осуществляется сбор и обработка данных.

Также в процессе проведения комплекса мероприятий по проверке уровня безопасности осуществляется анализ эффективности системы защиты сетевого и компьютерного оборудования рассматриваемой организации. Одновременно с этим осуществляется комплексная проверка всего ПО, установленного на этом оборудовании [3].

Сплошной проверке подлежат все объекты, на которых имеются носители информации. Это различные серверные стойки и информационные хранилища.

Составление отчета о проделанной работе с комплексной оценкой текущего состояния уровня информационной безопасности.

Этот этап проводимых работ предусматривает определение основного комплекса работ по устранению выявленных недостатков и слабых мест системы защиты информации.

Формирование отчетной документации на основании полученных результатов.

Документ содержит систематизированные результаты проведенной проверки, которые отражают сильные и слабые стороны системы обеспечения информационной безопасности. После изложения этой

информации дается перечень рекомендаций по совершенствованию текущего уровня безопасности информационных ресурсов сети. В результате проведения комплекса мероприятий по проверке уровня безопасности организация заказчик работ получает исчерпывающую информацию о текущем состоянии информационной безопасности и о потенциальных угрозах со стороны злоумышленников [14].

Выводы по Главе 1

В первой главе выпускной квалификационной работы проведено исследование теоретических аспектов обеспечения информационной безопасности объектов здравоохранения.

В данной главе произведен анализ литературных источников по теме исследования. Исследуемая тематика достаточно широко освещена в литературных источниках.

Произведен анализ основных понятий информационной безопасности и базовых принципов ее обеспечения. В завершении главы произведен анализ нормативно-правового обеспечения в области информационной безопасности.

В данный момент законодательная база, касающаяся обеспечения защиты информации в РФ, находится в состоянии формирования. Однако процесс ее развития и совершенствования происходит значительными темпами.

Глава 2 Исследование особенностей технического и программно-аппаратного устройства, угроз и уязвимостей информационной безопасности объекта – государственное бюджетное учреждение «Курганская больница скорой медицинской помощи»

2.1. Исследование особенностей технического и программно-аппаратного устройства медицинских организаций ГБУ «Курганская БСМП»

Выпускная квалификационная работа выполнена на базе Государственного бюджетного учреждения «Курганская больница скорой медицинской помощи» (ГБУ «Курганская БСМП»).

Организация ГБУ «Курганская БСМП», г. Курган, зарегистрирована 21 ноября 2002 года, ей были присвоены ОГРН 1024500519614, ИНН 4501027272 и КПП 450101001, регистратор – Инспекция Федеральной налоговой службы по г. Кургану. Юридический адрес организации – 640021, Курганская область, г. Курган, ул. Кирова, д. 65. Основным видом деятельности является: «Деятельность больничных организаций». Это старейшее лечебное учреждение в Курганской области.

Для достижения указанной цели Учреждение осуществляет следующие основные виды деятельности:

– медицинская деятельность;

– фармацевтическая деятельность;

– деятельность по обороту наркотических средств, психотропных веществ и их прекурсоров, культивированию наркосодержащих растений;

– деятельность, связанная с использованием источников ионизирующего излучения (генерирующих), в том числе их эксплуатация и хранение;

– деятельность, связанная с использованием возбудителей инфекционных заболеваний, микроорганизмов Ш-1/ групп патогенности;

– иные виды деятельности, направленные на достижение цели создания Учреждения.

На рисунке 2 представлена структура исследуемой медицинской организации.

Для рассматриваемой структуры приемное отделение включает:

– справочное бюро;

– приемные боксы;

– процедурные кабинеты.

Для рассматриваемой структуры имеются:

– инфекционное боксированное отделение респираторных инфекций;

– педиатрическое отделение;

– психоневрологическое отделение;

– хирургическое отделение;

– оториноларингологическое отделение.

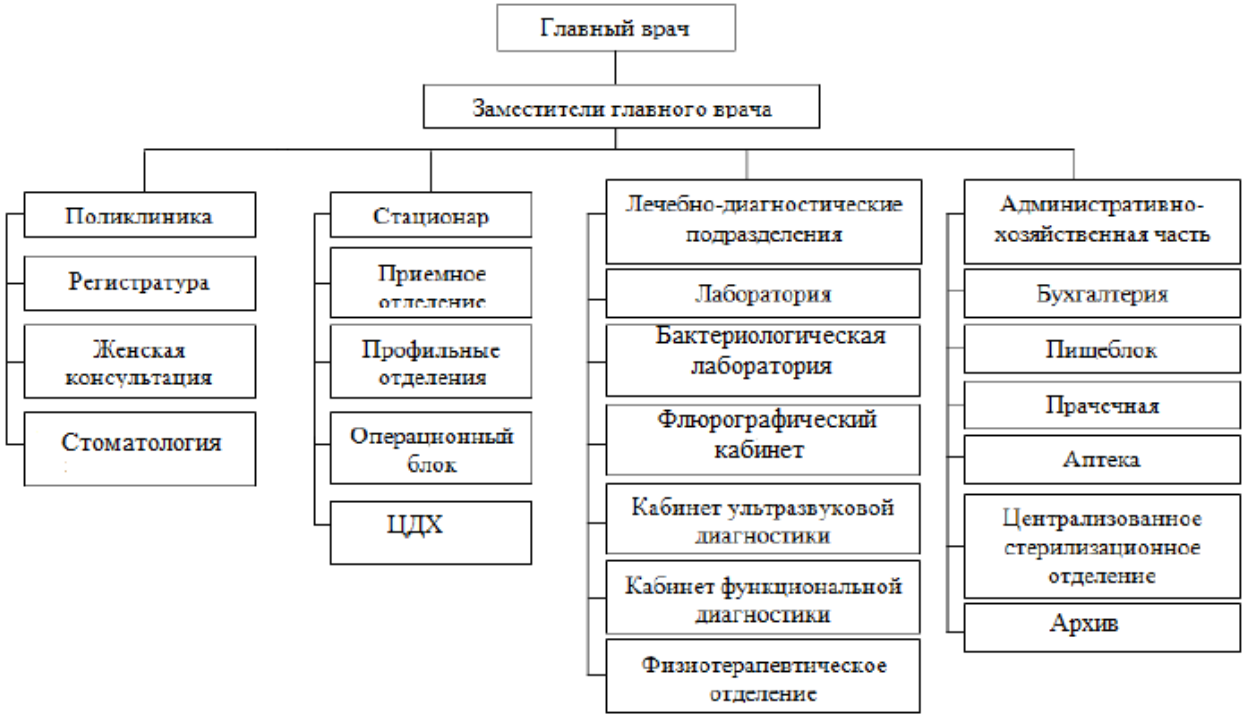

Рисунок 2 – Типовая структура медицинской организации

Операционный блок включает:

– предоперационная;

– операционная;

– послеоперационная.

Отделение анестезиологии – реанимации включает:

– палаты реанимационные для новорожденных детей;

– палаты реанимации и интенсивной терапии.

Травматолого-ортопедическое отделение для оказания плановой и экстренной амбулаторной круглосуточной помощи детскому населению включает:

– кабинеты врачей-травматологов-ортопеда;

– кабинет наложения гипсовых повязок;

– кабинет антирабических прививок.

С целью обеспечения высокого уровня безопасности информационных ресурсов рассматриваемой организации разработаны и введены в действие ряд руководств, требований и прочих нормативных документов, регулирующих информационную безопасность [15].

Правила работы с информационными ресурсами, представляющими собой персональные данные клиентов и сотрудников при их обработке на средствах ЭВМ.

Основные правила обеспечения информационной безопасности:

– организация разграничения сотрудников организации по наличию у них тех или иных прав доступа к персональным данным;

– разграничение прав доступа к защищаемой информации, хранящейся на информационных ресурсах организации.

Правила и ограничения работы сотрудников в сети Интернет и при отправке электронной почты.

Организация контроля за соблюдением требований к системе защиты персональных учетных данных с помощью паролей и ключей.

Контроль за соблюдением полого перечня требований, указанных в

инструкциях и правилах работы с персональными данными.

Составление и систематическая актуализация перечня документов и данных, которые входят в реестр документации.

Система информационной безопасности рассматриваемой организации представляет собой комплекс организационных и аппаратных средств защиты персональных данных. Для того, чтобы был обеспечен необходимый уровень защиты информационных ресурсов необходимо выполнение ряда задач, а именно:

- комплекс работ по организации и систематизации базы с персональными данными, а также контроль доступа к данной базе со стороны сотрудников, имеющих различные права доступа;
- систематический контроль соблюдения всего комплекса требований безопасности при работе с персональными данными;
- систематическое проведение инструктажей по правилам работы с защищаемой информацией среди всего персонала организации и проверка остаточных знаний с аттестацией и присвоением форм допуска к защищаемой информации;
- организация доступа персонала организации к защищаемой информации с использованием программного обеспечения, обеспечивающего разграничение пользователей на основе наличия у них прав доступа;
- проведение комплекса профилактических мероприятий, направленных на исключение вероятности несанкционированного доступа к защищаемой информации, а также ее утечки вследствие активности злоумышленников;
- формирование комплексного подхода к решению задач обеспечения информационной безопасности и защиты персональных данных [15, 16].

Существует несколько вариантов организации разграничения доступа персонала организации к персональным данным:

– с помощью программного обеспечения Alpha Internel, которое контролирует локальный трафик;

– с помощью программного обеспечения Sigma External, которое контролирует сетевой трафик.

Основным антивирусным программным обеспечением в рассматриваемой организации является ПО «Kaspersky». С помощью этого антивируса осуществляется постоянный мониторинг текущего уровня безопасности информационных баз. Эта антивирусная программа представляет собой эффективное средство защиты от большинства угроз безопасности информационных ресурсов в виде вредоносных подпрограмм и атак на систему безопасности. Основным преимуществом этой антивирусной программы является низкая требовательность к ресурсам и возможность работы в фоновом режиме без негативного влияния на быстродействие системы. Антивирус «Kaspersky» может быть установлен на большинство наиболее распространенных операционных систем.

Основными специфическими особенностями антивирусной защиты «Kaspersky» являются:

– эффективность работы на ПК, которые уже имеют вирусные программы и заражены вредоносным ПО. Данная особенность является самым важным преимуществом среди аналогов;

– при необходимости данное антивирусное программное обеспечение можно запускать без предварительной установки на ПК;

– при необходимости антивирусную защиту «Kaspersky» можно эффективно использовать после того, как она была установлена на ПК, которые уже инфицированы вредоносным ПО;

– программа подразумевает систематическую проверку наличия обновлений в сети Интернет на официальном сайте производителя.

В состав информационных баз данных объектов здравоохранения входят следующие документы: личные медицинские карты и истории болезней пациентов, отчетная документация о результатах деятельности

больниц и поликлиник [16].

Несмотря на то, что в медицинской сфере накопилось достаточно большое количество проблем, которые связаны с недостатком финансирования, цифровизация и автоматизация работы с документами в настоящее время находится на достаточно высоком уровне.

Под информационными технологиями подразумевается комплекс различных средств и инструментов, которые предназначены для работы с информационными ресурсами. Эти технологии подразумевают применение различных алгоритмов и принципов, в соответствии с которыми происходит обработка информации.

Современные информационные технологии имеют достаточно большой потенциал, который в полной мере раскрывается при работе с большими базами данных. Медицинская сфера и здравоохранение характеризуются большими и разветвленными базами данных.

Медицинские информационные системы начали внедряться сравнительно недавно. С их появлением медицина начала переходить на систему цифрового документооборота. Процесс перехода медицинских учреждений на цифровой документооборот подразумевает проведение большого объема работ по оцифровке документов. Таким образом все ранее используемые бумажные источники информации теперь имеют электронную копию.

После оцифровки документов, для удобства работы с ними, их необходимо определенным образом структурировать. С появлением баз данных возникла необходимость разработки средств, осуществляющих управление этими базами.

Современные информационные технологии в медицинской сфере позволяют осуществлять интерактивную поддержку пациентов. Другими словами, на основании имеющихся данных о диагнозе пациента, система в состоянии определить необходимый набор препаратов для лечения. Однако ввиду несовершенства этой системы, конечное принятие решения остается

за человеком.

Информационные технологии позволяют осуществлять прием и передачу информации между абонентами, которые находятся на больших расстояниях. Это свойство активно используется в медицинской сфере. В настоящее время стремительно развивается направление, называемое телемедициной. Телемедицина подразумевает взаимодействие между лечащим врачом и пациентом с помощью компьютерных технологий – видеосвязи. Таким образом, пациенту не обязательно посещать медицинское учреждение для того, чтобы получить консультацию врача [17].

Стоимость информационных технологий во многом определяет скорость их распространения и развития в медицинской сфере. Обширность сферы применения информационных технологий тем уже, чем выше их стоимость на рынке. При появлении того или иного продукта на рынке информационных технологий приводит к резкому скачку спроса на него. Еще совсем недавно для того, чтобы измерить артериальное давление или температуру тела человеку необходимо было прибегать к медицинскому оборудованию. Сейчас это и многое другое можно сделать с помощью смартфона или умных часов. При наличии специального программного обеспечения, которое имеется в открытом доступе, каждый человек может контролировать динамику изменения тех или иных показателей здоровья.

Планируется, что при всеобщей доступности к таким информационным технологиям в скором будущем вся собираемая информация о состоянии здоровья человека будет систематизироваться и отправляться в специальные базы данных. На основании этих данных информационные системы будут осуществлять анализ получаемой информации и оповещать человека в случае возникновения риска заболевания или развития каких-либо патологий.

В настоящее время в некоторых больницах и поликлиниках уже имеется все необходимое для того, чтобы осуществлять сбор информации о

текущем состоянии пациента дистанционно. На тело пациента устанавливаются необходимые датчики, которые считывают необходимые параметры. Эта информация передается в медицинское учреждение. Врач анализирует эту информацию и делает вывод о состоянии здоровья пациента.

В настоящее время существует большое количество различных аппаратных и компьютерных комплексов, которые являются представителями информационных технологий. С помощью этих комплексов проводится обучение и практическая отработка профессиональных навыков среди студентов хирургических специальностей [18].

МИС qMS представляет собой программный продукт, с помощью которого осуществляется управление медицинскими учреждениями. С помощью этого программного продукта реализуется возможность объединения большого количества организаций в единую компьютерную сеть. В базовый набор функций МИС qMS входит:

- электронная регистратура;
- личный кабинет пациента;
- ЭМК (электронная медкарта пациента);
- листы и журналы назначений;
- расписание ресурсов клиники;
- лист ожидания;
- стационар;
- лечебное питание;
- аптека, склад препаратов;
- центральное стерилизационное отделение;
- введение стандартов оказания врачебной помощи;
- экспертиза временной нетрудоспособности;
- экспертиза качества оказания медицинской помощи;

– управление финансами;

– расчеты по ОМС;

– отчетность;

– профилактика и диспансеризация;

– инструменты административного управления медицинской организацией (МО).

Далее необходимо изучить примеры практического применения различных информационных технологий для организации работы МИС.

Функция автоматизированной электронной регистратуры подразумевает оформление и регистрацию пациентов в медицинском учреждении путем внесение основной информации о нем в электронную базу данных, которая является аналогом регистратуры. Заполнение данных осуществляется по форме или шаблону, который состоит из необходимых разделов, в состав которых входят различные личные данные пациента [19].

Электронная регистратура может дополняться сторонними базами данных с различной информацией. Например, это может баз данных с информацией о полисах медицинского страхования пациентов. При вводе в электронную регистратуру идентификационных данных пациента, происходит поиск информации о нем по всем подгруженным базам данных. При наличии большого количества информации о пациенте из баз данных, оператор имеет возможность выбора именно той информации, которая ему необходима. При наличии в базах данных той или иной информации, она может заполняться в личную карту пациента в автоматическом режиме.

Также электронная регистратура позволяет на основании какой-либо информации из загруженных баз данных осуществлять идентификацию пациента. Например, при вводе номера полиса система автоматически осуществляет поиск электронной карты пациента, которому принадлежит данный полис.

Таким образом, информация о том или ином пациенте в случае необходимости может быть доступна медицинскому персоналу любого

здравоохранительного учреждения. Это очень удобно, так как человеку может понадобиться медицинская помощь в любое время и в любом месте, где бы он ни находился.

На каждого пациента заводится личная электронная карта, в которой хранится вся информация о нем и о истории его болезней и обращений в медицинские учреждения. Также эта карта содержит все данные о лабораторных исследованиях пациента и его организма. В дальнейшем планируется провести оцифровку всех медицинских документов, вплоть до самых первых записей, которые были сделаны еще в роддоме [20].

Врач в процессе работы с пациентами обрабатывает их персональными электронными медицинскими картами. Пациент имеет возможность обращения за медицинской помощью в любой точке страны, так как его электронная карта доступна в любом медицинском учреждении.

Наличие функции структурированного ввода данных в значительной степени облегчает работу медицинского персонала. У каждого специалиста имеется индивидуальная форма электронной карты, в которой помимо общей информации о пациенте, имеются данные, необходимые именно для этого медицинского специалиста.

МИС qMS способна при наличии соответствующих разрешений, автоматически осуществлять сбор всей имеющейся информации о пациенте из различных информационных баз, которые входят в состав единой системы. При наличии какой-либо медицинской информации о пациенте на сервере, система автоматически подгружает ее в электронную карту.

Все записи и отметки в электронной медицинской карте заверяются электронными подписями, которые имеются у каждого медицинского специалиста. При этом применяется система криптографической многоступенчатой защиты.

Несмотря на то, что рассмотренные примеры использования информационных технологий в медицине являются самыми простыми и базовыми, их наличие кардинально меняет степень удобства и

эффективности работы медицинского персонала в лучшую сторону [21].

2.2 Угрозы и уязвимости информационной безопасности ГБУ «Курганская БСМП»

На современном этапе развития компьютерных технологий и способов информационного взаимодействия наблюдается резкий рост значимости информации во всех отраслях и сферах жизнедеятельности. Для всех информационных баз, как личных, так и общественных, очень важна безопасность и надежная защита от вредоносного ПО и попыток несанкционированного доступа к личным данным пользователей. Так как к информационным ресурсам в электронном виде намного легче дистанционно получить несанкционированный доступ, они намного сильнее подвержены атакам вирусного ПО. При организации электронных информационных баз необходимо комплексно решать задачу ее надежной защиты, так как цифровые базы данных характеризуются легкостью и удобством их использования [22].

Далее необходимо провести более подробный анализ результатов деструктивного воздействия.

Первый класс воздействий состоит из [23]:

– уменьшения производительности комплекса программно-аппаратных средств;

– формирования ложных аппаратных и физических неполадок в процессе функционирования комплекса программно-аппаратных средств;

– переадресации информационных сообщений;

– взлома системы.

Основными целями несанкционированного доступа к информации автоматизированных систем являются [24]:

– взлом учетных записей пользователей;

– утечка конфиденциальных данных;

– получение базы паролей, которые необходимы для доступа к данным.

Одной из самых опасных разновидностей воздействия программных закладок является несанкционированная модификация информационных ресурсов. Это воздействие является причиной большого количества негативных последствий.

Социальная инженерия, в контексте информационной безопасности, относится к психологической манипуляции над людьми с целью заставить их совершить необходимые действия или разгласить конфиденциальную информацию. Отличительной особенностью данной атаки заключается в том, что она является одним из множества шагов более сложной схемы мошенничества [27].

Существует несколько наиболее основных и распространенных видов угроз относительно доступности СУБД:

– наличие у ключей доступа определенных признаков и свойств, повышающих степень их эффективности, а именно признак целостности и уникальности;

– функция защиты данных и информационных носителей от несанкционированного внесения изменений. При наличии такой угрозы злоумышленники смогут временно ограничить доступ пользователю к информационным ресурсам;

– неэффективное использование ресурсов ПК.

Классификация нарушителей и угроз безопасности информации приведена на рисунках 3 и 4.

Рисунок 3 – Классификация нарушителей безопасности информации

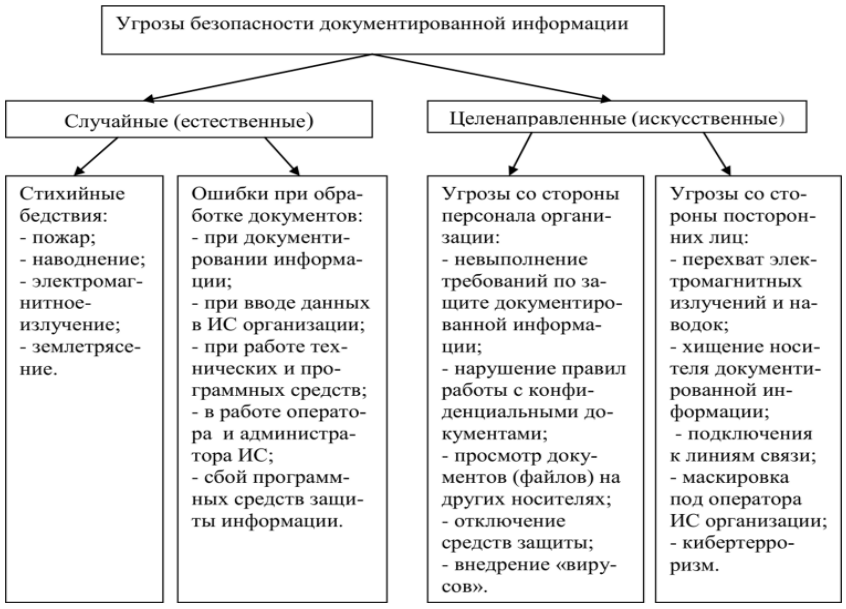

Рисунок 4 – Угрозы безопасности конфиденциальной информации

Наиболее эффективным способом выявления потенциальных угроз и наиболее уязвимых мест в системе информационной защиты является моделирование возможных сценариев хакерских атак на систему защиты информации. После моделирования потенциальных угроз и оценки их последствий осуществляется анализ наиболее подходящих средств и способов защиты информационных ресурсов сети организации [29].

2.3 Анализ существующих методик обеспечения комплексной информационной безопасности в медицинских учреждениях

Для эффективного решения задач обеспечения информационной безопасности в распределённых системах контроля технологических процессов существует структура методик и моделей противодействия – рисунок 5.

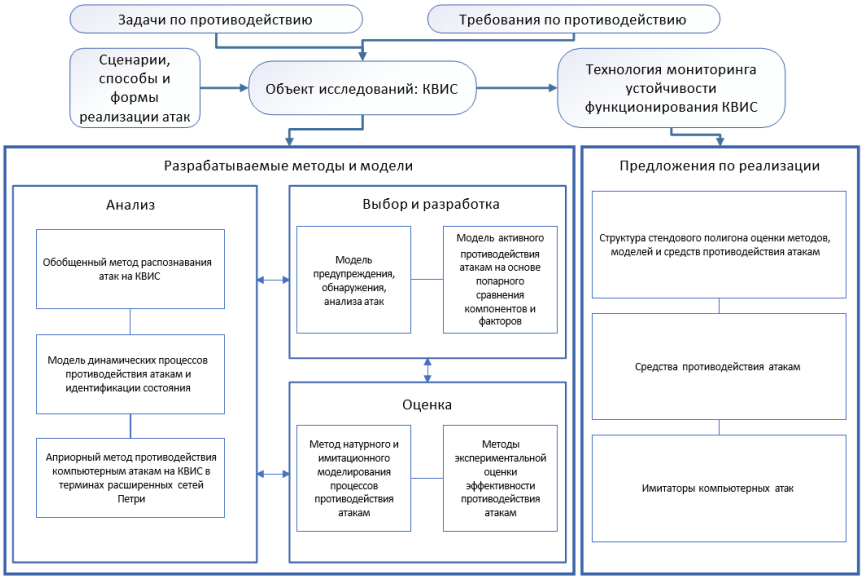

Рисунок 5 – Структура методов и моделей противодействия компьютерным атакам

Методики и модели, которые входят в состав данной структуры, должны соответствовать комплексу требований [13]:

– возможность оценки сценариев;

– мониторинг текущего состояния ТКС;

– профилактика возможных нарушений и анализ атак в соответствии с правилами и законами математики и логики.

Области применения популярной системы «Форпост» приведены в таблице 5.

Таблица 5 – Области применения системы «Форпост»

Область применения СОА Форпост	Класс защищенности
Автоматизированные системы по классификации ФСТЭК России	1В, 1Г, 2Б, 3Б, 1Д
Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных в соответствии с Приказом ФСТЭК России № 21	УЗ1, УЗ2, УЗ3, УЗ4
Защита информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей с Приказом ФСТЭК России № 31	К1, К2, К3
Защита информации, не составляющей государственную тайну, содержащейся в государственных информационных системах (ГИС) в соответствии с Приказом ФСТЭК России № 17	К1, К2, К3, К4

Данные системы должны иметь определенный уровень устойчивости к воздействию атак.

Выводы по 2 главе

Вторая глава выпускной квалификационной работы посвящена исследованию особенностей технического и программно-аппаратного устройства, угроз и уязвимостей информационной безопасности исследуемого медицинского учреждения.

В данной главе исследованы особенности технического и программно- аппаратного устройства систем контроля технологических процессов в медицинской сфере. Произведен анализ угроз и уязвимостей информационной безопасности распределённых медицинских систем.

В завершении главы произведен анализ существующих методик обеспечения информационной безопасности в распределённых информационных системах.

Глава 3 Разработка методики обеспечения комплексной информационной безопасности в ГБУ «Курганская БСМП»

3.1. Разработка типовой модели угроз информационной безопасности медицинской организации

Применяемые в настоящее время системы информационно защиты характеризуются высокой степенью удобства и возможности адаптации под конкретного пользователя. Вместе с этим данные системы характеризуются высокой степенью вероятности утечки защищаемой информации. С целью обеспечения комплексной защиты, которая отвечает всем современным требованиям необходимо обеспечить защиту системы от всех известных потенциальных угроз безопасности информационных ресурсов [31].

В настоящее время все имеющиеся потенциальные угрозы безопасности информационных ресурсов имеют следующую классификацию:

– слабые места в системе защиты информации и несовершенство противовирусных программ;

– противоправные действия, направленные на нарушение целостности информационных баз с целью несанкционированного доступа к защищаемой информации;

– противоправные действия относительно системы защиты информации со стороны сотрудников организации;

– использование устаревших и не эффективных средств противовирусной защиты;

– маскировка применяемого вредоносного ПО под штатное программное обеспечение, используемое на ПК с целью несанкционированного доступа к базе данных;

– вредоносное ПО, способное полностью или частично вывести из строя какую-либо часть системы информационной безопасности;

– воздействие на безопасность информационной базы средств промышленного шпионажа и хищения информации [32].

После выявления потенциальных угроз информационной безопасности необходимо определить вероятность возникновения каждой из потенциальных угроз, а также вероятные последствия и возможный ущерб.

При использовании локальных сетей и информационных баз имеется риск потери данных и доступ к ним злоумышленников с помощью вредоносного ПО. Очень важно комплексно осуществить анализ и оценку потенциальных рисков для целостности и сохранности информационных баз организации. Данная задача решается на этапе анализа уязвимостей информационных ресурсов. Также этот этап называется процедурой оценки возможных угроз.

Под угрозой подразумевается наличие потенциальной опасности, которая может стать причиной хищения защищаемой информации. Угроза является причиной того, что информационная база может быть подвержена атаке или повреждению, в результате чего часть данных будет утеряна или доступна третьим лицам [33].

С целью обеспечения комплексной защиты, которая отвечает всем современным требованиям необходимо обеспечить защиту системы от всех известных потенциальных угроз безопасности информационных ресурсов.

В настоящее время все имеющиеся потенциальные угрозы безопасности информационных ресурсов имеют следующую классификацию:

– противоправные действия относительно системы защиты информации со стороны сотрудников организации;

– вредоносное ПО, способное полностью или частично вывести из строя какую-либо часть системы информационной безопасности;

– слабые места в системе защиты информации и несовершенство противовирусных программ;

– маскировка применяемого вредоносного ПО под штатное программное обеспечение, используемое на ПК с целью несанкционированного доступа к базе данных;

– противоправные действия, направленные на нарушение целостности информационных баз с целью несанкционированного доступа к защищаемой информации;

– использование устаревших и не эффективных средств противовирусной защиты;

– воздействие на безопасность информационной базы средств промышленного шпионажа и хищения информации [34].

В связи с тем, что в современных условиях информационные ресурсы представляют собой особую ценность, они подвержены большому количеству различных угроз, которые могут иметь место как по одиночке, так и в комплексе. Именно поэтому и необходимо классифицировать и структурировать потенциально опасные факторы.

После выявления потенциальных угроз информационной безопасности необходимо определить вероятность возникновения каждой из потенциальных угроз, а также вероятные последствия и возможный ущерб.

Основным инструментом защиты информационных баз от несанкционированного доступа являются системы защиты, которые реализуют функции разграничения прав доступа, а также контролируют наличие в сетевом трафике потенциально опасных и вредоносных программ. Помимо этого, в состав систем информационной безопасности входят аппаратные средства защиты информационных ресурсов [35].

С целью обеспечения качественной и полноценной защиты информационных баз при работе в сети Интернет необходимо комплексное применение как программных, так и аппаратных средств защиты.

Основным условием обеспечения высокого уровня защиты информационных ресурсов сети предприятия является строгое соблюдение

правил и рекомендаций применяемой системы защиты информации. Разработка стратегии информационной безопасности организации начинается с полноценного и системного анализа наиболее вероятных и потенциальных рисков, которые могут стать причиной утечки информации.

Под термином стратегии безопасности подразумевается система мероприятий, направленная на обеспечение высокого уровня защиты информационных ресурсов с применением различных аппаратных и программных инструментов.

После разработки системы защиты данных и информационной безопасности разрабатывается политика безопасности, которая представляет собой комплекс правил, применимых всеми пользователями информационных ресурсов защищаемой сети. Как правило, разработка политики безопасности лежит в сфере ответственности службы безопасности, а также руководства предприятия.

Для обеспечения должного уровня защиты информационной системы все правила и рекомендации, которые содержатся в политике безопасности, должны выполняться всеми сотрудниками организации без исключения.

Политика безопасности представляет собой комплекс правил, применимых всеми пользователями информационных ресурсов защищаемой сети. Как правило, разработка политики безопасности лежит в сфере ответственности службы безопасности, а также руководства предприятия.

Информационная безопасность подразумевает выполнение комплекса требований, которые являются обязательными для всех пользователей сети. В первую очередь, пользователи должны систематически менять пароли доступа к учетным записям. Также руководство организации должно систематически проводить проверки выполнения требований политики безопасности сотрудниками организации. При таком комплексном подходе обеспечивается высокий уровень безопасности информационной сети и баз данных организации [36].

Политика безопасности разрабатывается на основе преследуемых целей, которые стоят перед службой информационной безопасности. Цель политики безопасности – это набор мероприятий, которые должны обеспечить требования относительно степени защиты информационных баз. Мероприятия могут иметь различный характер, например, организационные, программные, аппаратные и т. д. при каждом изменении структуры или состава информационной базы необходимо обновлять и адаптировать действующую политику безопасности. Постоянное обновление политики безопасности позволяет учитывать все актуальные и новые потенциальные угрозы.

Перед начальником службы информационной безопасности должны стоять четкие задачи и цели по обеспечению информационной безопасности. Существует несколько категорий целей и задач обеспечения информационной защиты:

– обеспечение безопасности информационных ресурсов сети;

– обеспечение эффективной системы процедур аутентификации;

– обеспечение эффективной системы процедур авторизации;

– обеспечение эффективной системы процедур контроля целостности ИБ;

– обеспечение эффективной системы процедур контроля конфиденциальности;

– систематическая проверка соблюдения требований политики информационной безопасности.

Все уровни информационной защиты должны строится в четком соответствии с поставленными целями и задачами. Основным условием эффективности системы информационной защиты является соответствие между целями и политикой информационной безопасности. При соблюдении этого условия обеспечивается максимальный уровень защиты баз данных от несанкционированного доступа.

В процессе формирования системы информационной безопасности

необходимо учитывать все факторы и риски. Еще одним важным условием является экономическая эффективность системы безопасности. Ее итоговая стоимость не должна превышать стоимости ущерба в случае реализации всех потенциальных угроз.

Политика безопасности в процессе ее проектирования и создания, подлежит полному документированию с фиксацией всех проведенных работ и затраченных на это средств. Также необходимо разработать комплекс рекомендаций по дальнейшей модернизации политики безопасности в соответствии с вновь появляющимися условиями и требованиями. Политика безопасности должна подлежать расширению, модернизации и адаптации под вновь возникшие условия и требования [37].

В процессе эксплуатации служба безопасности может выявить уязвимые места в системе безопасности. Для их устранения должны иметь место необходимые ресурсы и возможности, которые закладываются на этапе проектирования. При возникновении новых угроз, их устранение должно происходить как можно быстрее.

Обучение персонала и контроль их знаний политика безопасности – важнейший этап комплексной защиты информационных ресурсов. Для этой цели проводятся систематические занятия и проверки знаний.

Все уровни информационной защиты должны строится в четком соответствии с поставленными целями и задачами. Основным условием эффективности системы информационной защиты является соответствие между целями и политикой информационной безопасности.

В связи с тем, что для информации, составляющей коммерческую тайну, отсутствует методика определения актуальных угроз, в качестве основы принимается методика выявления перечня потенциальных опасностей относительно безопасности персональных данных. Выбранная методика имеет основу базовой модели угроз безопасности персональных данных [38].

Базовая модель содержит информацию о перечне потенциальных

опасностей. В типовых моделях угроз в базовой модели [5] рассматриваются автоматизированные рабочие места (АРМ), локальные и распределенные информационные системы, которые имеют возможность доступа к сетям общего пользования.

Угрозы НСД, в свою очередь, включают в себя угрозы в зависимости от варианта типовой модели угроз (Приложение А, Таблица А.1). К рассматриваемой ИС можно отнести один из шести вариантов базовой модели угроз [5]:

– типовая модель угроз безопасности информации, обрабатываемой в АРМах, не имеющих подключения к открытым сетям;

– типовая модель угроз безопасности информации, обрабатываемой в АРМах, имеющих подключение к открытым сетям;

– типовая модель угроз безопасности информации, обрабатываемой в локальных ИС, не имеющих подключения к открытым сетям;

– типовая модель угроз безопасности информации, обрабатываемой в локальных ИС, имеющих подключение к открытым сетям;

– типовая модель угроз безопасности информации, обрабатываемой в распределенных ИС, не имеющих подключения к открытым сетям;

– типовая модель угроз безопасности информации, обрабатываемой в распределенных ИС, имеющих подключение к открытым сетям.

Видовая информация может быть взломана путем применения средств оптического отображения на различных электронных устройствах и средствах вычислительной техники.

Существуют следующие пути утечки видовой информации:

– удаленный доступ к экранам дисплеям;

– создание видео-аппаратных закладок.

Существуют следующие пути утечки информации через каналы ПЭМИН:

– побочные электромагнитные излучения электронных вычислительных средств;

– создание помех в цепях питания;

– формирование источников радиоизлучений, которые передают модулированные сигналы.

Нарушители являются потенциальными источниками несанкционированного доступа к базам данных. Они могут получить доступ к информационным системам, к пользовательским данным. Также существуют нарушители, у которых отсутствует возможность прямого доступа к информационным системам. Они создают угрозы со стороны сетей связи, которые предназначены для общего пользования. Существует два типа нарушителей [39]:

– внешние нарушители;

– внутренние нарушители.

Если потенциальная угроза реализуема в рассматриваемой информационной системе и является потенциально опасной для базы данных, то ее можно рассматривать как актуальную. Существует методика, в соответствии с которой происходит формирование списка актуальных угроз. Данная методика описывается в основных правилах по выявлению актуальных угроз безопасности [4].

В процессе выбора наиболее оптимальных и эффективных средств и инструментов защиты необходимо руководствоваться таким термином, как «классификация системы». Существует несколько признаков и критериев, по которым производится классификация. Такой подход позволяет относительно быстро и правильно относить тот или иной инструмент защиты к какому-либо классу. В качестве примера можно привести автоматизированные средства работы с базами данных, в которых основными классификационными признаками являются руководящие документы [40]. В случае работы с персональными данными основным руководящим документом является Постановление правительства №1119, которое регламентирует процедуры обеспечения безопасности личной информации. Для работы с информационными системами, в состав которых

входят документы, относящиеся к секретным и не имеющим в своем составе персональных данных, необходимо использовать классификационные признаки «1Г» или «1Д». Действующий в настоящее время комплект нормативно – правовой документации, регулирующий вопросы классификации систем автоматизированного документооборота, не имеет в своем составе актов, которые учитывали бы такие средства защиты данных, как антивирусное ПО и средства виртуализации. Эти средства защиты конфиденциальной информации определены соответствующими приказами ФСТЭК. Таким образом, для создания современной и эффективной системы информационной защиты необходимо учитывать и эти инструменты в процессе моделирования потенциальных угроз.

Существует определенный перечень документов, в соответствии с которыми осуществляется анализ потенциальных рисков относительно баз данных конфиденциальной информацией.

Основной руководящий акт, согласно которому осуществляется анализ потенциальных рисков и угроз для конфиденциальной информации был принят ФСТЭК России в 2021 году. После введения этого документа довольно сильно изменились требования к моделированию потенциальных угроз и формированию требований относительно систем защиты информационных баз. Это объясняется тем, что в этом документе были учтены все современные потенциальные риски и средства для их противодействия.

До недавнего времени основными методиками выявления наиболее опасных рисков для информационных систем были:

– методика выявления наиболее опасных факторов для обрабатываемой конфиденциальной информации при использовании специализированных систем для работы с такими данными;

– методика выявления наиболее опасных факторов для обрабатываемой конфиденциальной информации при использовании ключевых систем и объектов информационной инфраструктуры.

Данные методические рекомендации имеют довольно ограниченное применение в связи с тем, что они относятся к категории узкоспециализированных и в настоящее время потеряли свою актуальность.

Новые методические рекомендации предназначены для обеспечения информационной безопасности следующих объектов:

– системы хранения данных;

– системы информационного взаимодействия с различной степенью автоматизации;

– сети передачи телекоммуникационных сигналов;

– объекты инфраструктуры массовой информации и распространения телекоммуникационных данных;

– системы облачного хранения информации.

Согласно новым методическим рекомендациям, процедура анализа угроз информационной безопасности состоит из следующих этапов:

– анализ возможного ущерба в результате реализации той или иной угрозы или комбинации угроз;

– анализ наиболее вероятных объектов атак злоумышленников;

– анализ возможности реализации тех или иных угроз на основании данных об используемых средствах защиты информации оценка возможности реализации (возникновения) угроз безопасности информации.

Описанный выше этап подразумевает реализацию трех отдельных шагов, состав которых приведен ниже [41].

Идентификация основных потенциальных опасностей базам данных. Согласно новому принципу анализа потенциальных угроз, методика не предусматривает анализ рисков, которые обусловлены непосредственными действиями злоумышленников. В связи с этим рассматриваемая методика не содержит целого ряда обстоятельств, которые не относятся к так называемому человеческому фактору:

– действие различных природных факторов в виде стихий и природных катаклизмов;

– наличие уязвимых мест в системе криптографических инструментов защиты информации;

– потенциальная опасность утечки конфиденциальной информации через технические каналы.

Необходимо иметь ввиду тот факт, что при составлении модели информационных угроз включение в ее состав тех или иных факторов происходит после обязательного согласования их с теми людьми, которые являются владельцами защищаемой информации, а также с операторами локальных сетей [42].

Результатами анализа потенциальных опасностей для баз данных являются:

– определение основных видов и инструментов атаки на защищаемые информационные ресурсы со стороны злоумышленников;

– определение основных категорий потенциальных злоумышленников по различным критериям.

Анализ инструментов и способов несанкционированного доступа к защищаемой информации.

В рамках этого этапа происходит определение:

– основных категорий и видов злоумышленников, которые относятся к числу наиболее потенциальных и вероятных;

– основных способов и инструментов, применяемых с целью атаки на базы данных, в том числе и применяемого ПО.

Определение наиболее актуальных рисков для информационной безопасности.

Основными признаками актуальных и потенциальных угроз являются:

– наличие четко выраженного объекта, на который может осуществляться атака;

– наличие одного или нескольких потенциальных нарушителей информационной безопасности;

– наличие путей несанкционированного доступа к информационным

базам;

– наличие значимого ущерба при реализации выявленных угроз.

Актуальность рассматриваемой угрозы информационной безопасности считается высокой в случае выявления способов ее реализации. Все выявленные потенциальные угрозы должны быть тщательно проанализированы на предмет их реализации. Способы и пути реализации угроз анализируются на основе имеющихся данных о тактике поведения злоумышленников. Если был выявлен хотя бы один способ реализации угрозы, она относится к категории актуальных и вносится в создаваемую модель потенциальных рисков.

Согласно новой системе рекомендаций все выявленные угрозы и способы их реализации вносятся в состав формируемой модели в соответствии с определенной структурой. По мере развития информационных технологий и совершенствования системы защиты информации данные рекомендации должны постоянно актуализироваться.

Для проведения комплексного исследования и анализа потенциальных угроз могут привлекаться как собственные силы и ресурсы, так и ресурсы сторонних профильных организаций. Организации, осуществляющие подобные виды деятельности не должны в обязательном порядке иметь соответствующие лицензии и сертификаты на проведение таких работ. на определенном этапе формирования данной системы регламентов предполагалось, что такие организации будут сертифицироваться и лицензироваться, однако в последствии было решено отказаться от этой идеи. Это объясняется тем, что подобные виды услуг не подлежат обязательной сертификации и лицензированию [43].

Современная методика обладает рядом преимуществ, среди которых:

– применимость для решения широкого спектра задач;

– наличие большого количества справочной информации и обучающего материала;

– наличие большого количества информации о правилах

эффективного использования экспертного метода;

– наличие большого количества инструментов для эффективного выявления всех потенциальных рисков и угроз.

Если потенциальная угроза реализуема в рассматриваемой информационной системе и является потенциально опасной для базы данных, то ее можно рассматривать как актуальную. Существует методика, в соответствии с которой происходит формирование списка актуальных угроз. Данная методика описывается в основных правилах по выявлению актуальных угроз безопасности [4]. В первую очередь проводится анализ реализуемости рассматриваемой актуальной угрозы. Эти особенности представлены в таблице, которая содержится в методических указаниях по формированию перечня актуальных угроз [44]. В соответствии с табличными данными информационная система представляет собой систему, в состав которой имеются коммерческие данные. Таблица 3.1 содержит информацию о показателях исходной защищенности, в соответствии с которыми осуществляется процедура выбора и расчета условий исходной защищенности.

Вероятность возникновения угрозы – показатель, который рассчитывается по определенной методике и характеризующий степень опасности взлома доступа [4] к информационным ресурсам сети. Показатели исходной защищенности информационной системы показаны в таблице 6.

Таблица 6 – Показатели исходной защищенности информационной системы

Основные параметры информационной системы	Степень надежности		
	Хорошая	Удовлет-ворительная	Неудо-влетвори-тельная
Возможность подключения к общедоступным информационным сетям: Информационная система с возможностью подключения к множеству общедоступных информационных сетей;	–	–	+
Информационная система с возможностью подключения к одной общедоступной информационной сети;	–	+	–
Информационная система с отсутствием возможности подключения к общедоступным информационным сетям	+	–	–
Наличие интегрированных операций: считывания информации, поиска информации;	+	–	–
Сортировки информации, удаления информации, записи информации	–	+	–
Преобразования информации	–	–	+
Ограничение прав доступа клиентов сети: Информационная система с ограниченным количеством лиц, имеющих доступ к ее ресурсам	–	+	–
Информационная система, не имеющая каких-либо ограничений доступа к ее ресурсам	–	–	+
Информационная система, которые характеризуются открытым доступом для всех клиентов	–	–	+

Таблица 7 содержит информацию о всех угрозах, которые могут возникнуть в рассматриваемом случае. При этом принимается во внимание то факт, что информационная система имеет доступ в сеть Интернет.

Таблица 7 – Оценка вероятности реализации угрозы безопасности

Наименование потенциальной опасности	Степень опасности угрозы								Итоговое значение
	Специалисты ОТП	локальные пользователи	удаленные пользователи	АБИ сегмента ИС	системные администраторы	АБИ ИС	Специалисты ОППО	специалисты СТОиРО	
	K_1	K_2	K_3	K_4	K_5	K_6	K_7	K_8	Y_2
Несанкционированный доступ к ресурсам сети до загрузки операционной системы и во время	10	2	0	10	10	10	5	10	7

загрузки									
Несанкционированный доступ к ресурсам сети после загрузки операционной системы	0	0	0	10	10	10	10	0	5
Несанкционированный доступ к ресурсам сети с целью анализа сетевого трафика	0	0	5	5	5	5	5	0	3
Несанкционированный доступ к ресурсам сети с целью анализа внутреннего трафика сети	0	2	0	5	5	5	5	0	3
Несанкционированный доступ к ресурсам сети с целью сканирования параметров информационной системы	0	0	5	5	5	5	5	0	3
Несанкционированный доступ к ресурсам сети с целью удаленного использования приложений	0	0	2	0	10	0	0	0	2
Несанкционированный доступ к ресурсам сети с целью установки вредоносного ПО	0	10	0	10	10	10	10	0	6

Формула для расчета коэффициента реализуемости угрозы имеет следующий вид:

$$Y = (Y_1 + Y_2)/20 \quad (1)$$

В соответствии с величиной коэффициента реализации для каждой угрозы осуществляется формирование вербальной интерпретации согласно следующему неравенству:

$$0 \leq Y \leq 0{,}3 \quad (2)$$

В этом случае вероятность реализации угрозы является низкой.

$$0{,}3 < Y \leq 0{,}6 \quad (3)$$

В этом случае вероятность реализации угрозы является средней.

$$0{,}6 < Y \leq 0{,}8 \quad (4)$$

В этом случае вероятность реализации угрозы является высокой.

$$Y > 0{,}8 \quad (5)$$

В этом случае вероятность реализации угрозы является очень высокой [4].

С целью определения степени актуальности каждой из угроз, перечисленных в таблице 7, применяется экспертный метод. Согласно этой

методике каждой угрозе присваивается определенный уровень опасности: высокий, средний или низкий.

Аналогичным образом осуществляется проведение экспертной оценки в соответствии с рассматриваемой методикой. Этот показатель представляет собой вербальный параметр, который может принимать три различных значения – таблица 8.

Таблица 8 – Значение показателей опасности

Степень угрозы	Характеристика и признаки
Низкая	При возникновении угрозы имеется низкая вероятность наступления масштабных последствий
Средняя	При возникновении угрозы имеется средняя вероятность наступления масштабных последствий
Высокая	При возникновении угрозы имеется высокая вероятность наступления масштабных последствий

На основании известных угроз проведем оценку актуальности угроз в таблице 9.

Проведя анализ данных, представленных в таблице 9 можно сделать вывод, что актуальными угрозами исследуемой больницы являются:

– несанкционированный доступ к ресурсам сети до загрузки операционной системы и во время загрузки;

– несанкционированный доступ к ресурсам сети после загрузки операционной системы;

– несанкционированный доступ к ресурсам сети с целью анализа сетевого трафика;

– несанкционированный доступ к ресурсам сети с целью сканирования параметров информационной системы;

– несанкционированный доступ к ресурсам сети с целью установки вредоносного ПО.

Таблица 9 – Оценка актуальности угроз

Наименование потенциальной опасности	Возможность реализации	Опасность угроз	Актуальность угрозы
Несанкционированный доступ к ресурсам сети до загрузки операционной системы и во время загрузки	очень высокая	высокая	актуальная
Несанкционированный доступ к ресурсам сети после загрузки операционной системы	высокая	высокая	актуальная
Несанкционированный доступ к ресурсам сети с целью анализа сетевого трафика	высокая	низкая	актуальная
Несанкционированный доступ к ресурсам сети с целью анализа внутреннего трафика сети	высокая	низкая	актуальная
Несанкционированный доступ к ресурсам сети с целью сканирования параметров информационной системы	высокая	низкая	актуальная
Несанкционированный доступ к ресурсам сети с целью удаленного использования приложений	средняя	низкая	неактуальная
Несанкционированный доступ к ресурсам сети с целью установки вредоносного ПО	высокая	высокая	актуальная

Для перечня угроз, составленного выше необходимо определить эффективные способы противодействия, способные свести к минимуму вероятность их возникновения.

3.2 Разработка типовой модели нарушителя информационной безопасности медицинской организации

Существует следующая классификация потенциальных нарушителей целостности и безопасности информационных баз, которые представляют ту или иную степень опасности:

– внешние нарушители, у которых отсутствуют возможности легального проникновения на территорию организации;

– внутренние нарушители, у которых имеется возможность систематического или единичного доступа на территорию организации.

Под нарушителями подразумеваются лица, способные нанести вред целостности информационных баз, а также осуществит

несанкционированный доступ к информационным ресурсам, представляющим собой конфиденциальную информацию [6].

По мере того, как происходит развитие организации и увеличение штата ее сотрудников, растет и число каналов коммуникации между другими организациями. В связи с этим, неизбежно растет и вероятность возникновения тех или иных видов угроз информационным базам организации. Основной целью злоумышленников являются именно каналы распространения и обмена данными как внутри организации, так и между ними [45].

Под термином злоумышленник подразумевается субъект, осуществляющий незаконную деятельность с целью получения несанкционированного доступа к конфиденциальной информации. При достижении своих целей злоумышленник нарушает целостность информационных ресурсов, и они могут стать доступными третьим лицам. К злоумышленникам могут относится как отдельные лица, так и группы лиц, действия которых направлены на незаконное хищение информации. Также существуют лица, осуществляющие промышленный шпионаж и относящиеся к различным структурам разведки, безопасности и т. д.

В различных ситуациях и в зависимости от целей злоумышленников, в случае хищения какого-либо носителя информации может иметь место утрата конфиденциальности данных, которые находятся на данном носителе информации. В ряде случаев хищение носителя информации может и не сопровождаться утратой конфиденциальности данных. Также существуют ситуации, при которых утрата данными конфиденциальности не связана с хищением носителя информации.

Вследствие каких-либо ошибочных действий со стороны пользователя имеет место непреднамеренное воздействие на безопасность информационных ресурсов. Также к категории непреднамеренного воздействия относятся различные явления природного характера, способные оказать негативное воздействие на работоспособность и

надежность носителей информации.

В случае преднамеренного хищения или порчи информации имеет место определенный интерес к ней со стороны злоумышленников. Как только информация начала передаваться по каким-либо каналам связи, для ее безопасности возникает определенная потенциальная опасность. Как правило, передача документов осуществляется для того, чтобы провести необходимые согласующие и утверждающие мероприятия.

Существует определенная классификация основных видов угроз конфиденциальной информации: угрозы функционального характера, временные угрозы, угрозы различного масштаба, угрозы организационного характера.

Угрозы функционального характера также имеют классификацию: они могут быть потенциальными и реальными. В свою очередь реальные функциональные угрозы подразделяются на пассивные и активные [46].

Временные угрозы могут быть периодическими, постоянными, а также эпизодическими.

В зависимости от масштабности угрозы могут быть локальными или глобальными.

Угрозы организационного характера могут быть либо спланированными заранее, либо носить случайный характер реализации во времени.

Особую опасность рассмотренные выше угрозы представляют для документов, хранящихся в электронном виде. Это связано с тем, что в ряде случаев достаточно сложно своевременно вывить факт несанкционированного доступа к документам. Угроза информационной безопасности – это какие-либо действия со стороны злоумышленников, которые направлены на нарушение целостности и прочих характеристик безопасности информационных ресурсов. В результате реализации угрозы информация может стать доступной для третьих лиц, которые используют ее в преступных целях [9].

Наиболее распространенными угрозами для электронной документации являются:

– хищение носителя информации злоумышленниками;

– незаконный доступ к электронным документам с целью их хищения или порчи;

– незаконное копирование информации, которая является конфиденциальной;

– замена оригинального носителя данных на аналогичный, который не является местом хранения оригиналов документации;

– несоблюдение правил работы с документами, содержащими персональные данные;

– несанкционированное копирование данных с носителей информации с помощью различных массивов.

Существует несколько путей нарушения безопасности персональных данных и конфиденциальной информации. В одном случае хищение или несанкционированный доступ к данным может иметь место в процессе работы с ней. В другом случае такая ситуация может возникнуть при обработке электронных документов с применением нового программного обеспечения, степень защиты которого изучена не в полной мере. Наиболее часто второй путь нарушения безопасности персональных данных и конфиденциальной информации имеет место в процессе формирования различных баз данных и прочих компонентов хранения и обработки информационных ресурсов [47].

В настоящее время самыми популярными и эффективными инструментами несанкционированного доступа к персональным данным являются различные программно-аппаратные средства. С помощью этих средств осуществляется работа с данными.

Существует следующая классификация потенциальных нарушителей целостности и безопасности информационных баз, которые представляют ту или иную степень опасности:

– внешние нарушители, у которых отсутствуют возможности легального проникновения на территорию организации;

– внутренние нарушители, у которых имеется возможность систематического или единичного доступа на территорию организации.

Компьютерные вирусы представляют собой самые распространенные и вредоносные программные средства для несанкционированного доступа к данным и хищения информации.

С помощью компьютерных вирусов злоумышленники осуществляют взлом информационных баз с целью получения незаконного доступа к данным. Вирусы встраиваются в программное обеспечение и нарушают работу системы безопасности и защиты.

Еще одним довольно распространенным средством деструктивного воздействия на информационные базы и персональные данные являются программные закладки, а также алгоритмические закладки.

Существует классификация основных видов воздействий на информационные базы со стороны средств деструктивного воздействия:

– нарушение алгоритмов функционирования как программных, так и аппаратных компонентов системы;

– нарушение системы защиты и безопасности информационных ресурсов с целью получения несанкционированного доступа; работа с базами данных с целью внесения в их состав и структуру каких-либо изменений.

Таким образом, очевидно, что закладки являются наиболее опасным и распространенным инструментом деструктивного воздействия на защищаемые базы данных. Помимо этого, алгоритмические и программные закладки способные вносить изменения в алгоритмы управления работой аппаратной части информационных систем и баз данных.

Внешним нарушителем информационной безопасности в настоящей модели, является нарушитель, не имеющий прямого доступа к техническим средствам локальной вычислительной сети, находящимся в пределах

контролируемой зоны ИС [48].

В настоящей модели вводится предположение, что внешний нарушитель имеет возможность действовать на защищаемые данные в локальной вычислительной сети исключительно в процессе передачи информации по каналам данной сети.

Возможности внутреннего нарушителя в значительной степени зависят от воздействующих в пределах локальной вычислительной сети ограничений, основное из которых – это реализация комплексной организационно- технической защиты.

Классификация типов нарушителей относительно возможностей доступа к компонентам узлов информационной системы приведены в таблице 10.

Таблица 10 – Типы нарушителей информационной безопасности

Характеристика нарушителя	Тип
Внешний нарушитель	Тип 1
Пациент	Тип 2
Обслуживающий персонал	Тип 3
Сотрудник, не являющийся пользователем	Тип 4
Оператор	Тип 5
Администратор	Тип 6
Сотрудник организации, обслуживающей ТС и ПО	Тип 7

Предположения о средствах атак, которые имеются у нарушителя, приведены в таблице 11.

Таблица 11 – Предположения об имеющихся средствах атак

Средства атак	Возможность использования средства атак
Аппаратные компоненты криптографической защиты	Отсутствует
Технические средства, а также программное обеспечение	Возможно применение данных средств (включая компьютерные вирусы)
Целенаправленно разработанные технические средства, а также программное обеспечение	Отсутствует
Штатные средства	Штатные средства размещаются в пределах контролируемой зоны
Средства атак	Возможность использования средства атак
Распределенные ресурсы различных сетей	Возможна организация атак
Средства перехвата, а также обработки информационных ресурсов в кабельном или коммуникационном оборудовании	Возможно применение

Система разграничения прав доступа в ИС гарантирует разграничение прав пользователей ИС на доступ к различным видам ресурсов ИС в соответствии с действующей политикой ИБ.

С целью формализации модели нарушителя предлагается использовать специально разработанную таблицу. Данная таблица заполняется непосредственно после анализа модели угроз и политики безопасности компании. В формировании данной таблицы принимают участие экспертная группа, в состав которой входят представители службы безопасности компании.

3.3 Формирование методики обеспечения комплексной информационной безопасности в ГБУ «Курганская БСМП»

Целью разработки методики обеспечения информационной безопасности является обеспечение устойчивого функционирования систем в разрезе стандартного функционирования и в случаях непрерывного негативного воздействия атак. Данная цель позволяет определить подход к разработке методик противодействия негативному влиянию атак, при котором появляется необходимость обеспечить взаимосвязанность устойчивости и защищенности функционирования распределенных систем.

Основные требования к методике аудита приведены ниже.

Разрабатываемая методика должна быть применима к организационно- штатной структуре компании и должна определять роли сотрудников, участвующих в проведении самооценки ИБ (внутреннего аудита).

Разрабатываемая методика должна определять последовательность действий, выполняемых в рамках аудита ИБ.

Методика аудита ИБ должна определять распределение полномочий, ответственность и обязанности участников аудита, в том числе устанавливать необходимость привлечения специализированных сторонних организаций для проведения внешнего аудита и вовлеченность подразделений компании для проведения внутреннего аудита.

Методика аудита ИБ должна устанавливать периодичность проведения аудитов.

Методика аудита ИБ должна определять порядок и форму документальной фиксации результатов аудита.

В процессе проведения проверки эффективности информационной безопасности необходимо составить план необходимых мероприятий и масштаб исследования. Перед началом проведения работ обоими сторонами оговариваются все нюансы предстоящих работ. Таким образом сводится к

минимуму вероятность возникновения спорных моментов после завершения работ. Процесс проведения проверки эффективности информационной безопасности подразумевает выполнение следующих операций:

– формирование коллектива, который будет осуществлять работу по проведению оценки эффективности;

– определение зоны ответственности для каждого члена команды;

– необходимый набор исходной информации, которая будет использоваться при проведении проверки эффективности информационной безопасности;

– состав объектов, с которыми будут проводиться работы по проверки эффективности информационной безопасности;

– перечень потенциально возможных угроз и нарушителей информационной безопасности организации;

– последовательность действий в процессе проведения проверки эффективности информационной безопасности и необходимое для этого время.

Проведение аудита безопасности корпоративной информационной системы компании осуществляется в четыре этапа:

Первый этап. Постановка задачи, уточнение границ работ.

Второй этап. Сбор и анализ информации.

Третий этап. Проведение анализа рисков.

Четвертый этап. Разработка рекомендаций.

Более подробное описание каждого этапа аудита информационной безопасности описывается далее.

Постановка задачи, уточнение границ работ. Данный этап включает сбор необходимых исходных данных, проведение их предварительного анализа, проведение организационных мер, касающихся подготовки проведения аудита информационной безопасности, а именно:

– Уточнение целей и задач аудита ИБ.

– Формирование рабочей группы для проведения аудита ИБ.

– Подготовка и согласование технического задания на проведение аудита ИБ.

Анализ информационных ресурсов компании. Проводится анализ характеристик ИС:

– Организационных характеристик;

– Организационно-технических характеристик;

– Технических характеристик, которые связаны с архитектурой информационной системы;

– Технических характеристик, которые связаны непосредственно с конфигурацией устройств сети и серверов информационной системы;

– Технических характеристик, которые связаны с функционированием механизмов информационной безопасности.

Когда все исходные данные получены, компания-исполнитель формирует отчет об обследовании, который предоставляется комиссии, сформированной от компании-заказчика. Данный отчет является базой для следующих уровней аудита ИБ – анализ рисков и разработка рекомендаций по улучшению ИБ компании.

Процедура проведения анализа информационных рисков. Данный этап – это очень важная стадия аудита информационной безопасности компании. Процедура анализа рисков производится с целью оценить реальные угрозы нарушения режима защиты информации и формирования предложений, выполнение которых даст возможность минимизировать данные угрозы безопасности информации. Исходная информация для анализа информационных рисков – это согласованный с компанией-заказчиком отчет о произведенном обследовании.

Процедура анализа рисков позволяет:

– произвести адекватную оценку существующих угроз информационной безопасности компании;

– произвести идентификацию критичных ресурсов

информационной системы;

– произвести выбор адекватных требований в области обеспечения ЗИ;

– разработать перечень самых опасных уязвимых направлений и угроз.

В процессе анализа рисков информационной безопасности производят:

– классификацию информации компании;

– анализ уязвимостей компании;

– составление модели возможного злоумышленника;

– оценку рисков нарушения ИБ.

При проведении анализа рисков должны произвести, в том числе и оценку степени критичности уязвимых мест, а также возможности использования этих мест возможными злоумышленниками с целью осуществления противоправных действий.

Разработка рекомендаций. На основе данных, полученных в результате исследования информационной структуры, а также результатов анализа рисков информационных активов, должны быть разработаны некоторые решения. По завершению аудита формируется отчет, который содержит оценку исходного уровня безопасности информационных ресурсов, данные об имеющихся проблемах, а также анализ выявленных рисков информационной безопасности, рекомендации по устранению этих рисков.

Результаты проведения аудита в компании. Результатом аудита безопасности компании должен быть аудиторский отчет.

Общая структура отчета включает:

– оценку имеющегося уровня защищенности информационных ресурсов компании:

а) описание и оценка исходного уровня защищенности информационных ресурсов компании;

б) анализ конфигурации информации, анализ найденных уязвимостей;

в) анализ информационных рисков, которые могут быть связаны с возможностью реализации различных угроз ресурсам информационной системы компании;

– рекомендации относительно технических составляющих информационной безопасности:

– изменение конфигурации имеющихся технических сетевых устройств;

– изменение конфигурации имеющихся средств обеспечения информационной безопасности;

– активация дополнительных механизмов информационной безопасности системного ПО;

– использование дополнительных программных средств защиты информации;

– рекомендации относительно организационной составляющей информационной безопасности компании:

а) разработка политики информационной безопасности компании;

б) организация службы информационной безопасности;

в) разработка организационно-распорядительной и нормативно-технической документации;

г) пересмотр ролевых обязанностей персонала компании, а также зон ответственности сотрудников;

д) разработка программ осведомленности персонала в области защиты информации;

е) поддержка и повышение квалификации сотрудников.

Аудит информационной безопасности – независимая экспертная оценка защищенности информационной системы компании с учетом таких факторов как персонал, процессы и технологии.

Наибольшую опасность представляют атаки, которые могут стать

причиной нарушения функционирования системы. В связи с этим максимальный упор в процессе проведения аудита делается именно на такие угрозы – рисунки 6 и 7.

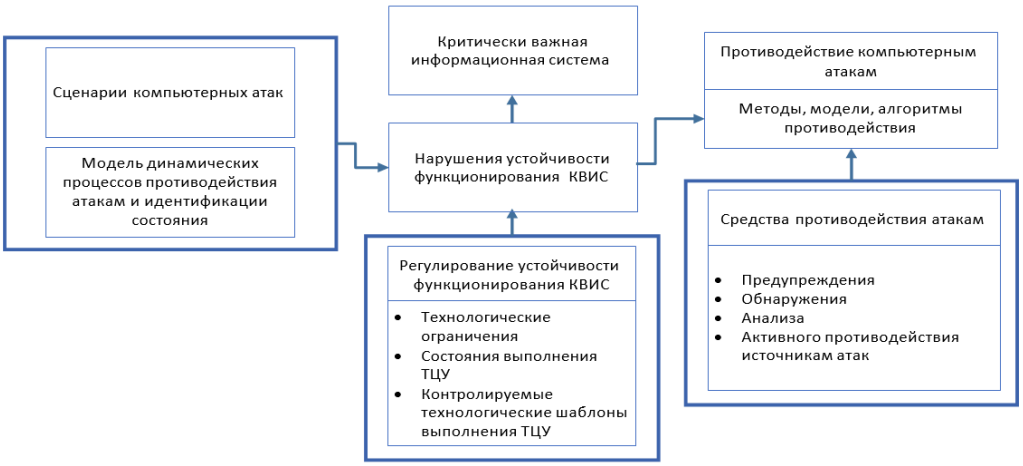

Рисунок 6– Обобщенная схема подхода к разработке аудита ИС

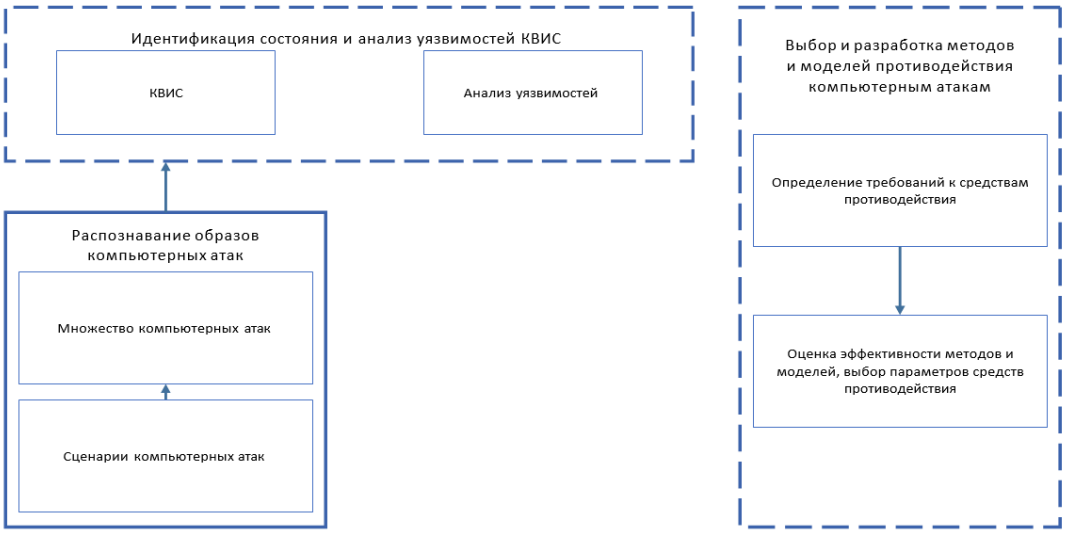

Рисунок 7 – Методическая схема противодействия атакам

Предназначенные для управления медицинскими процессами системы должны функционировать в соответствии с определенной схемой.

Для выявления угрозы внешних атак необходимо проведение сигнатурного и функционального анализа нештатных событий.

Исходя из вышесказанного, можно сделать вывод о том, что разработка методик и моделей по противодействию компьютерным атакам подразумевает:

– выбор комплекса параметров регулирования информационной системы; выбор методов, моделей и алгоритмов противодействия атакам;

–выбор средств предупреждения, обнаружения и анализа атак; проведение мероприятий по активному противодействию атакам.

Все эти мероприятия должны обеспечивать стабильность и устойчивость функционирования системы.

Качество методов эффективного выявления, профилактики и ликвидации последствий информационных атак в процессе аудита определяется применяемыми средствами противодействия компьютерным атакам. В состав этих средств могут входить элементы сигнатурного анализа, выявление аномалий, функциональный анализ исполняемых функций системы. Для достижения максимальной эффективности противодействия компьютерным атакам подразумевается применение модернизированного обобщенного комбинированного метода.

Распознавание атак в процессе функционирования системы подразумевает под собой анализ параметров информационно-вычислительного процесса в соответствии с заданными правилами выявления аномальных параметров. Теория распознавания образом в максимальной степени описывает комплекс процедур, необходимых в процессе противодействия атакам. Данная теория подразумевает интерпретацию объектов компьютерных атак в качестве распознаваемых образов пространства.

Формирование пространства признаков атак осуществляется в соответствии с априорными знаниями процессов эксплуатации и жизнедеятельности системы и согласно классификации атак. После этого производится уточнение апостериорной информации. Датчики средств противодействия относятся к основным источникам информации, при

помощи которых происходит распознавание объектов атак и потенциальных угроз их воздействия на систему.

Модель распознавания атаки на систему представлена на рисунке 8.

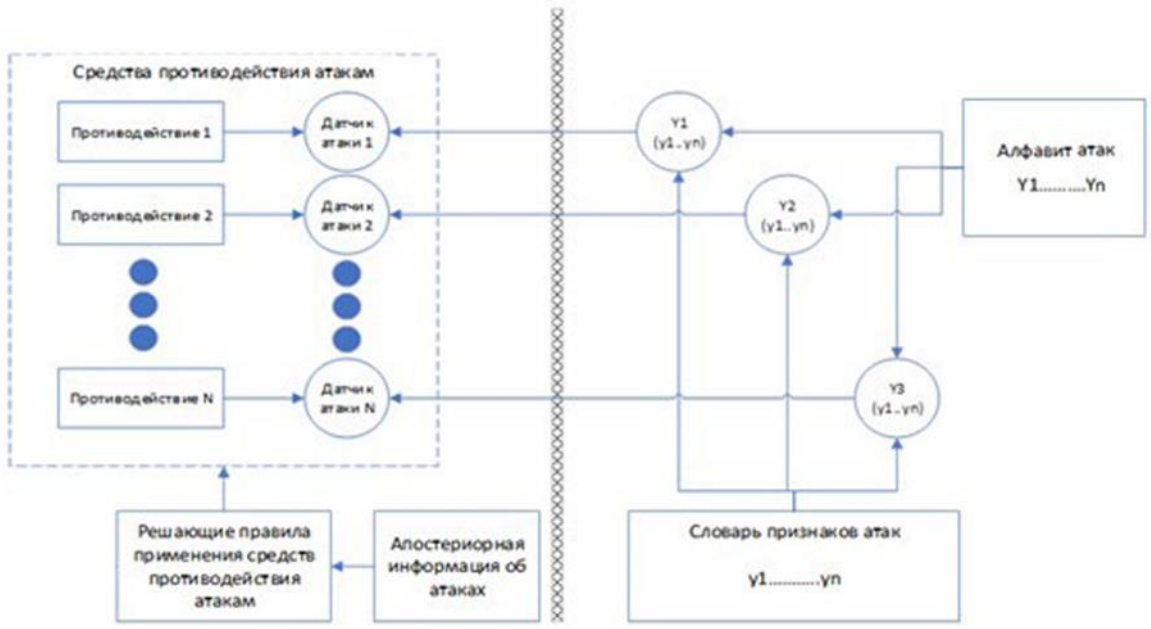

Рисунок 8 – Модель распознавания атаки на распределенную систему

Существует классификация основных признаков компьютерных атак:

– детерминированные признаки атак. Для их идентификации применяются сигнатурные методы обнаружения атак;

– вероятностные признаки атак. Для их идентификации применяются методы анализа аномальных отклонений;

– логические признаки атак. Для их идентификации используются методы функционального анализа.

Модель содержит апостериорную информацию. Она необходима для

определения возможности активации защитных алгоритмов, в основе которых лежит принцип изучения аномальных отклонений.

Инициализация попыток несанкционированного доступа осуществляется на основании данных, которые поступают от датчиков, с

помощью которых анализируется текущее состояние системы [13].

В процессе определения необходимого набора процедур для защиты системы комплекс создает априорный словарь, который содержит признаки и классификацию атак.

При отсутствии информации о классификации потенциальных атак, необходимо знать правила, с помощью которых можно идентифицировать атаки и осуществить их классификацию.

В случае уменьшение числа классов атак приводит к уменьшению ошибок при их распознавании.

3.4 Разработка практических рекомендаций по применению организационных, правовых и программно-аппаратных средств защиты информации в ГБУ «Курганская БСМП»

Основные результаты аудита ИБ ГБУ «Курганская БСМП» приведены ниже.

Физический контроль доступа в помещения офиса компании.

– текущее состояние: ограничение передвижения персонала, наличие системы пропусков;

– оптимизация структуры: доступ к зонам должен управляться и быть ограничен только полномочными лицами;

– нарушения и замечания: нет системы гибкого управления физическим доступом; отсутствие персональных идентификаторов; отсутствует анализ прав доступа в зоны безопасности;

– меры для исправления ситуации: регламентировать период проверки прав доступа в зоны безопасности; проводить согласно регламенту проверку прав доступа в зону безопасности;

Аппаратное обеспечение информационной системы компании.

– текущее состояние: открытый доступ к средствам обработки информационных ресурсов;

– оптимизация структуры: сетевые кабели должны быть защищены от неразрешенного перехвата или повреждения;

– нарушения и замечания: имеет место беспрепятственный доступ к коммутационному оборудованию;

– меры для исправления ситуации: обеспечить закрытие дверей коммутационных шкафов на замки.

Сетевое обеспечение информационной системы компании.

– текущее состояние: кабеля ЛВС находятся в доступном месте; в некоторых местах не защищены кабель-каналами;

– реорганизация организационной структуры: необходимо обеспечить защиту информации, передаваемой по кабельным линиям от перехвата; для этого используются экранированные кабели;

– выявленные недостатки: некоторые кабельные трассы не оснащены средствами защиты от утечки информации, на некоторых участках кабельных трасс силовые проводы проложены совместно с проводами, по которым передаются информационные сигналы;

– необходимые мероприятия по устранению выявленных недостатков: использование в сети более совершенных маршрутизаторов, обеспечивающих более высокую степень защиты информации.

ПО, предназначенное для организации системного функционирования.

– состояние на данный момент времени: на ПК организации используется ПО как с лицензией, так и бесплатные версии для общего доступа;

– мероприятия по улучшению: внедрение в рабочий процесс исключительно лицензированных версий ПО;

– выявленные недостатки: часть ПК в рассматриваемой организации работает с бесплатными пиратскими копиями ПО;

– необходимые мероприятия по устранению выявленных недостатков: внедрение в рабочий процесс исключительно

лицензированных версий ПО.

Прикладное программное обеспечение.

– состояние на данный момент времени: место расположения ссылок для запуска программного обеспечения – рабочий стол ПК; активированы функции автоматической блокировки; уровень надежности паролей соответствует требованиям;

– необходимые мероприятия по устранению выявленных недостатков: все ПК организации должны быть оснащены системой аутентификации пользователей; все ПК должны быть настроены таким образом, что при бездействии оператора ПК переходит в режим блокировки; все пароли на ПК должны соответствовать требованиям сложности и безопасности;

– нарушения и замечания: база без пароля;

– меры для исправления ситуации: установка паролей; по возможности использовать шифрование для важных документов.

Комплекс организационных мер.

– состояние на данный момент времени: часть используемого сетевого оборудования имеет незащищенный доступ; все пользователи сети имеют возможность применения съемных носителей информации; пароли части пользователей имеют открытый доступ для всех клиентов;

– выявленные недостатки: отсутствие жесткого регламента относительно применения съемных носителей информации; отсутствие курсов по изучению основных требований соблюдения мер предосторожности утечки информации; отсутствие жесткого регламента относительно работы удаленных рабочих столов;

– предлагаемые мероприятия по совершенствованию: внедрение жесткого регламента относительно применения съемных носителей информации; организация курсов по изучению основных требований соблюдения мер предосторожности утечки информации; внедрение жесткого регламента относительно работы удаленных рабочих столов;

– необходимые мероприятия по устранению выявленных недостатков: внедрение жесткого регламента относительно применения съемных носителей информации; организация курсов по изучению основных требований соблюдения мер предосторожности утечки информации; внедрение жесткого регламента относительно работы удаленных рабочих столов.

Корпоративные данные компании.

– текущее состояние: пользователи имеют неограниченный доступ к съёмным устройствам; получить доступ к корпоративным данным может любой пользователь;

– оптимизация структуры: наличие системы мониторинга пользователей;

– нарушения и замечания: отсутствует шифрование документов;

– меры для исправления ситуации: установка и конфигурирование системы мониторинга пользователей.

Выводы относительно проведенного аудита информационной безопасности.

В ходе проведенного аудита выявлены некоторые нарушения информационной безопасности компании на уровне физического и программного обеспечения безопасности. В соответствии с выявленными нарушениями даны рекомендации по их немедленному устранению.

Одним из первоначальных принципов является то, что организация расследования инцидентов информационной безопасности возлагается на подразделение информационной безопасности с привлечением при необходимости руководителей и сотрудников других подразделений. Создается комиссия, которая утверждается приказом. Данный приказ может отстранять на время от исполнения служебных обязанностей сотрудников в случае выявления сотрудником нарушений в части соблюдения установленных мер ИБ.

Расследование инцидентов. Данный факт необходим для

исследования возможности компрометации конфиденциальной информации, циркулирующей в организации в целом. Также при подобном нарушении необходимо исследование информационной безопасности на предмет спланированной системы по ее компрометации, направленной на хищение, модификацию или уничтожение данных конфиденциального характера.

В качестве основных источников информации об инцидентах информационной безопасности можно считать:

– ответственное лицо в обязательном порядке должно быть назначено соответствующим приказом руководителя организации;

– результаты функционирования средств мониторинга информационной безопасности, как и результаты проведения проверок и аудита, как внутреннего, так и внешнего;

– обращения сотрудников или иных лиц с заявлением на имя руководителя организации с указанием факта возникновения инцидента информационной безопасности и подробного его описания;

Необходимо понимать, что добросовестности сотрудников является едва ли не ключевым фактором в вопросах проведения расследования инцидентов информационной безопасности.

Любой из сотрудников может выявить признаки наличия инцидента информационной безопасности, анализируя текущую ситуацию на предмет ее соответствия утвержденным требованиям и концепции обеспечения безопасности предприятия, которая должна быть в обязательном порядке доведена под роспись всем должностным лицам. Выявленные несоответствия являются основанием для предположения о том, что возник инцидент информационной безопасности.

Если инцидент создал урон или возможности для его появления, но информацию об уроне получить не представляется возможным, организация расследования происходит в порядке и сроки, предусмотренные приказом руководителя организации.

Для перечня угроз, составленного выше необходимо определить эффективные способы противодействия, способные свести к минимуму вероятность их возникновения.

Таблица 12 содержит информацию о способах противодействия угрозам рассматриваемой сети.

Таблица 12 – Способы противодействия имеющимся угрозам

Способы защиты	Угрозы безопасности
СДЗ	Несанкционированный доступ к ресурсам сети до загрузки операционной системы и во время загрузки
СЗИ от НСД после загрузки	Несанкционированный доступ к ресурсам сети до загрузки операционной системы и во время загрузки Несанкционированный доступ к ресурсам сети после загрузки операционной системы
Антивирус	Несанкционированный доступ к ресурсам сети с целью установки вредоносного ПО
Построение зашифрованных каналов связи (межсетевой экран, VPN)	Несанкционированный доступ к ресурсам сети с целью сканирования параметров информационной системы Несанкционированный доступ к ресурсам сети с целью анализа сетевого трафика
Средства обнаружения сетевых вторжений (СОВ)	

На основании таблицы 3.7 в ИС медицинского учреждения можно сделать вывод, что наиболее эффективными средствами защиты будут являться:

- средство доверенной загрузки (СДЗ);
- СЗИ от НСД;
- средство антивирусной защиты САВЗ;
- защита каналов связи (межсетевой экран, VPN);
- средство обнаружения сетевых вторжений (СОВ).

Кратко рассмотрим некоторые программно-технические средства защиты на конкретных примерах.

Средство доверенной загрузки. Доверенная загрузка компьютера

необходима для того, чтобы воспрепятствовать несанкционированному запуску ПК лицами, которые могут представлять опасность для информационных ресурсов.

Для обеспечения высокого уровня защиты базы данных необходимо применять комплексный подход, который заключается в использовании нескольких инструментов (как программных, так и аппаратных). В настоящее время имеется множество комбинированных аппаратно-программных средств защиты информации.

Решено применить систему Аккорд-5.5.

Аккорд-5.5 оснащен функцией обесточивания ПК если в течении определенного количества времени после его включения не произошел запуск BIOS АМДЗ. С целью ограничения доступа к ПК в Аккорд-АМДЗ предусмотрена функция авторизации с помощью смарт-карт и других устройств идентификации пользователей [10].

СЗИ от НСД. Они могут быть представлены программными продуктами, техническими средствами и т.д. С их помощью осуществляется профилактика и защита взлома баз данных.

В настоящее время рынок представлен множеством различных средств защиты информации.

Средства защиты информации от несанкционированного доступа обладают широким функционалом, однако их основное назначение заключается в обеспечении:

– контроля доступа к базам данных со стороны пользователей;

– протоколирования фактов запуска и работы с приложениями пользователями сети;

– контроля обмена информацией между клиентами сети;

– ограничения доступа к базам данных со стороны клиентов, которые являются потенциальными путями утечки информации.

Наиболее популярными средствами защиты информации от НСД на сегодняшний день являются:

– Аккорд-Win 64K;

– Secret Net;

– Страж NT.

Рассмотрим более подробно перечисленные программные средства защиты информации.

Комплекс «Аккорд-Win64K» разработан для решения следующих задач: реализация функций проверки пользователей, осуществляющих попытки входа в сеть с целью получения доступа к базам данных и информационным ресурсам сети [7].

Данное ПО предназначено для работы со всеми операционными системами семейства Microsoft. ПО «Аккорд-Win64K» выполняет следующие функции [7]:

– исключение вероятности доступа к базам данных со стороны злоумышленников;

– контроль и проверка прав доступа к информационным ресурсам всех пользователей, осуществляющих попытку получения доступа к ресурсам сети;

– защита информационных ресурсов и баз данных от возможных повреждений вследствие сбоя в работе ЭВМ;

– общая защита программного обеспечения и операционной системы сети;

– профилактика изменения данных со стороны неавторизованных пользователей сети;

– формирование для каждого клиента сети отдельной рабочей области, утечка информации из которой исключена;

– контроль и предотвращение попыток работы с программными продуктами от недостоверных поставщиков;

– дискретизация прав доступа клиентов сети к базам данных с целью исключения вероятности утечки информации;

– мандатный принцип организации контроля доступа клиентов к

информационным ресурсам и базам данных сети;

– протоколирование всех фактов обмена информацией меду клиентами сети;

– применение программных модулей Аккорд и ПСКЗИ ШИПКА для контроля клиентов сети в процессе их работы с информационными ресурсами сети;

– обязательные процедуры авторизации для всех клиентов, которым необходим доступ к сети или серверам терминалов;

– дополнительные возможности по автоматизации авторизации при работе в ОС семейства Windows;

– автоматическая регистрация всех сессий работы в терминальных подсетях;

– протоколирование всех фактов применения носителей информации, подключаемых через USB.

Программный продукт «Secret Net» является одним из самых распространенных сертифицированных приложений, которое реализует функции защиты сетей от доступа со стороны злоумышленников. С помощью этого ПО выполняются все требования руководящих документов относительно безопасности данных и информационных ресурсов.

Программный продукт «Secret Net» выполняет следующие функции:

– контроль и проверка прав доступа к информационным ресурсам всех пользователей, осуществляющих попытку получения доступа к ресурсам сети;

– формирование для каждого клиента сети отдельной рабочей области, утечка информации из которой исключена;

– профилактика изменения данных со стороны неавторизованных пользователей сети;

– постоянный мониторинг безопасности каналов, по которым идет обмен конфиденциальными данными;

– протоколирование всех фактов применения носителей

информации, подключаемых через USB.

– при записи информации на носители осуществляется автоматическая проверка всей памяти устройства на наличие остаточных фрагментов;

– реализация функций непрерывного анализа информационных угроз со стороны злоумышленников;

– возможность изменения масштаба и сферы контроля системой для более эффективной работы в условиях большой нагрузки на сеть;

– возможность организации структуры сети в виде отдельных терминалов с функциями создания удаленных рабочих мест.

Программное обеспечение «Страж NT» разработано для решения задач по обеспечению комплексной безопасности баз данных компьютерных сетей и защиты от утечки информации.

Программный продукт «Страж NT» выполняет следующие функции:

– применение многоступенчатой системы доступа клиентов к ресурсам сети;

– необходимое применение аппаратных средств авторизации клиентов;

– дискретизация прав доступа клиентов сети к базам данных с целью исключения вероятности утечки информации;

– постоянный мониторинг уровня защиты информационных каналов сети;

– контроль и предотвращение попыток работы с программными продуктами от недостоверных поставщиков;

– протоколирование всех фактов обмена информацией меду клиентами сети;

– размещение на всех документах, которые выводятся на печать опознавательных знаком и специальных маркеров;

– функции защиты информационных ресурсов от их разделения с последующей дефрагментацией с целью хищения;

– обязательные процедуры авторизации для всех клиентов, которым необходим доступ к сети или серверам терминалов;

– контроль фактов применения носителей информации для обмена данными сети;

Рисунок 9 содержит схему, согласно которой функционируют СЗИ от НСД.

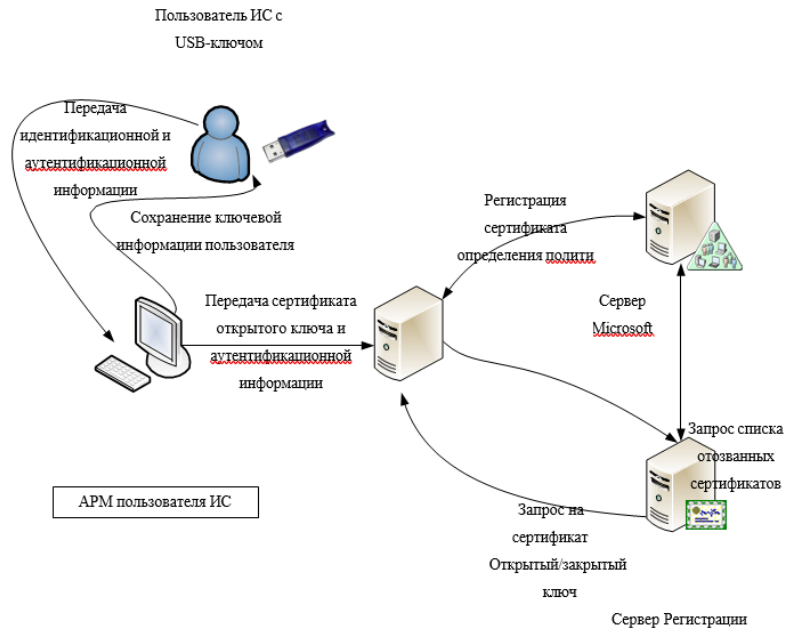

Рисунок 9 – Пример функционирования СЗИ от НСД

Средства антивирусной защиты информационной системы.

Произведем аналитическое сравнение наиболее популярных продуктов антивирусного программного обеспечения, которое присутствует на рынке ПО на сегодняшний день.

В течение последних лет особую актуальность приобрели вопросы об основных показателях эффективности бесплатного программного обеспечения, предназначенного для защиты данных от несанкционированного доступа и действия компьютерных вирусов. К основным показателям эффективности такого рода ПО относятся: удобство пользования, потребляемые ресурсов производительности ПК, способность противостоять действию вредоносного ПО.

Под бесплатным антивирусным программным обеспечением подразумевается программный продукт, обеспечивающий ту или иную степень защиты ПК от воздействия компьютерных вирусов и хакерских атак с целью хищения или получения несанкционированного доступа к личной и конфиденциальной информации. Такой вид ПО имеется в открытом доступе и может быть скачан бесплатно из сети Интернет. Особенность такого ПО заключается в том, что его использование не подразумевает прохождение активации и ввода специального ключа или пароля, которые необходимы для латных версий антивирусного ПО. С одной стороны, для многих пользователей очень удобно наличие в открытом доступе антивирусных программ, с другой стороны, бесплатные версии антивирусного ПО имеют достаточно ограниченный функционал, что сказывается на степени безопасности данных ПК или локальной компьютерной сети.

Достаточно часто можно встретить предложения крупных разработчиков антивирусного ПО предложений о бесплатной эксплуатации лицензионных копий при условии их совместного использования в рамках различных платформ, таких как Яндекс, Google и т.д. Далее проведем сравнительный анализ наиболее распространенных и эффективных бесплатных антивирусных программ.

Avast Free является лидером среди бесплатного ПО для защиты компьютеров и сетей от вредоносного ПО и компьютерных вирусов.

Основными достоинствами этого программного продукта являются:

– наличие русифицированного интерфейса;
– относительно низкие требования к производительности ПК;
– наличие инструментов защиты почтовых клиентов и браузеров;
– относительная простота эксплуатации.

К отрицательным сторонам Avast Free следует отнести нестабильность выпуска разработчиком баз обновлений для противодействия новым вирусам.

Microsoft Security представляет собой антивирусную бесплатную

программу, разработанную корпорацией MicroSoft. Данное антивирусное ПО отличается своей функциональностью при относительно простом интерфейсе и низкими требованиями к производительности ПК.

Основными достоинствами этого программного продукта являются:

– относительно простой интерфейс;

– простота настройки и отладки под конкретные условия эксплуатации и решаемые задачи;

– отсутствие большого количества оповещений и всплывающих окон.

К отрицательным сторонам следует отнести:

– ограниченный функционал;

– отсутствие инструментов защиты почтовых клиентов и браузеров;

– возможность использования исключительно с ОС Windows.

Это антивирусное ПО в наибольшей степени подходит для начинающих и не опытных пользователей ПК, которые достаточно редко пользуются сетью Интернет. Microsoft Security необходимо использовать совместно с инструментами защиты почтовых клиентов и браузеров.

Avira Antivirus представляет собой производительный и относительно мощный инструмент антивирусной защиты, имеющий русифицированный интерфейс и ориентированный на применение на домашних ПК. Несмотря на русскоязычный интерфейс, довольно часто самые последние обновления не русифицированы. Avira Antivirus характеризуется относительно высокими требованиями к производительности ПК, а также медленным сканированием системы на предмет наличия вирусов.

Программный продукт AVG: ANTI-VIRUS FREE обладает средним уровнем надежности и функционалом.

Основными достоинствами этого программного продукта являются:

– наличие русифицированного интерфейса;

– относительно простой интерфейс;

– наличие инструментов защиты почтовых клиентов и браузеров;

– наличие версий для мобильных устройств.

К отрицательным сторонам следует отнести:

– ограниченный функционал;

– необходимость наличия высокопроизводительного оборудования;

– высокий риск не обнаружения вирусной угрозы.

Далее произведем сравнительный анализ бесплатного антивирусного ПО Avast Free и двух программных продуктов, распространяющихся на платной основе - Kaspersky Antivirus и Kaspersky Internet Security.

Таблица 13 содержит результаты сравнения трех антивирусных продукта.

Таблица 13 – Основные характеристики антивирусного программного обеспечения

Функциональные показатели	KAV	KIS	Avast!Free
Монитор файловой системы (проверяет файлы на жестком диске в процессе работы)	есть	есть	есть
Монитор почты (проверка трафика почтовых программ)	есть	есть	есть
Веб-монитор (проверка веб-трафика и скриптов на открываемых страницах)	есть	есть	есть
Монитор интернет-чатов (ICQ, Mail.ru-агент и др.)	есть	есть	есть
Анти-фишинг (блокирует мошеннические сайты)	есть	есть	есть
Монитор поведения (определяет потенциально-опасные программы на основе их поведения)	есть	есть	есть
Песочница (виртуальная среда для запуска непроверенных приложений)	нет	есть	есть
Анти-спам (защита от спама)	нет	есть	нет
Сетевой экран – брандмауэр (защита от сетевых и хаккерских атак)	нет	есть	нет
Контроль программ (проверка репутации запускаемых программ)	нет	есть	нет

Наиболее продвинутые решения в данной области предлагает компания «Лаборатория Касперского».

Программно-аппаратные средства межсетевого экранирования. Рассмотрим несколько решений от компании Cisco:

– Cisco ASA5505-K8;

– Cisco ASA5510-K8;
– Cisco ASA5540-K8;
– Cisco ASA5580-20-BUN-K8.

С помощью программного продукта Cisco ASA 5500 Series сети защищены от утечки информации в соответствии с самым высоким классом защиты. Это обеспечивается за счет наличия очень широкого функционального набора этого ПО. В зависимости от имеющегося уровня нагрузки осуществляется выбор той или иной модели. Помимо этого, на выбор модели могут влиять такие факторы, как требуемое число интерфейсов, необходимость сканирования системы для выявления модулей сетевых вторжений.

В заключении будет произведена разработка проекта внедрения средств защиты информации в информационную архитектуру объекта.

Определим этапы выполнения проекта и длительность работы. Результаты представлены в таблице 14.

Таблица 14 – Трудоемкость и продолжительность работ по проекту

Наименование этапов разработки	Исполнители (должность)	Трудоём-кост ь, час	Продолжите льность, дней
1. Подготовительный этап			
1.1 Предварительный осмотр объекта	Специалист по внедрению	16	2
1.2 Анализ информационной составляющей предприятия	Специалист по внедрению	24	3
1.3 Анализ программной и технической составляющей предприятия	Специалист по внедрению	40	5
1.4 Изучение планов помещений, схем технических коммуникаций, связи и других документов	Специалист по внедрению, руководитель проекта	16	4

Продолжение таблицы 14

Наименование этапов разработки	Исполнители (должность)	Трудоём-кост ь, час	Продолжите льность, дней
1.5 Оформление результатов, полученных при проведении	Специалист по внедрению	16	2

осмотра помещений и объектов			
	Итого	112	16
2. Основной этап			
2.1 Подготовка и настройка оборудования	Специалист по внедрению, руководитель проекта	8	1
2.2 Проведение измерений	Специалист по внедрению, руководитель проекта	8	1
2.3 Разработка архитектуры ИС	Специалист по внедрению	8	1
2.4 Формирование списка необходимых технических средств	Специалист по внедрению, руководитель проекта	16	2
	Итого	40	5
3. Закупка необходимых технических средств			
3.1 Анализ рынка, поиск оптимальных поставщиков	Специалист по внедрению	24	3
3.2 Покупка оборудования	Специалист по внедрению, руководитель проекта	8	1
	Итого	32	4
4. Заключительный этап			
4.1 Коммутация оборудования	Специалист по внедрению	8	1
4.2 Пуско-наладочные работы, проверка функционирования системы	Специалист по внедрению, руководитель проекта	24	3
4.3 Экономическое обоснование работы	Специалист по внедрению	16	2
4.4 Составление отчетов и рекомендаций	Специалист по внедрению, руководитель проекта	8	1
	Итого	40	5
	Всего	224	28

Из таблицы 14 видно, что на разработку проекта и планирование его внедрения потребуется 28 дней. Теперь необходимо составить календарный план выполнения проекта. Календарный план дает возможность контроля над ходом выполнения работ, его регулирования на всех этапах работ.

План выполнения работ по данному проекту составлен в виде таблицы 15.

Таблица 15 – Календарный план разработки и реализации проекта

Наименование этапов	Период выполнения		Продолжитель-ность этапов, дн
	дата начала	дата окончания	
1. Подготовительный этап	16.07.2023	08.08.2023	14
2. Основной этап	09.08.2023	15.08.2023	5
3. Закупка необходимых технических средств	09.08.2023	12.08.2023	4
4. Заключительный этап	13.08.2023	17.08.2023	5
Итого			28

Комплексный этап внедрения проекта включает в себя следующие стадии:

– инициализация;

– установка;

– автоматизация деятельности;

– обучение сотрудников.

Эти стадии включают в себя все задачи проекта. Комплексный этап внедрения состоит из четырех процессов, изображенных на рисунке 10.

Под тестированием исходных данных понимают проверку являющейся основой для проведения экспертизы фотографической информации. Распознаваемые системой ситуации должны быть покрыты набором применяемых при тестировании данных.

Логическое тестирование. Под логическим тестированием понимают выявление логических ошибок в системе продукций – несогласуемых условий, конфликтных, избыточных и циклических правилах, то есть тех, которые не зависят от предметной области.

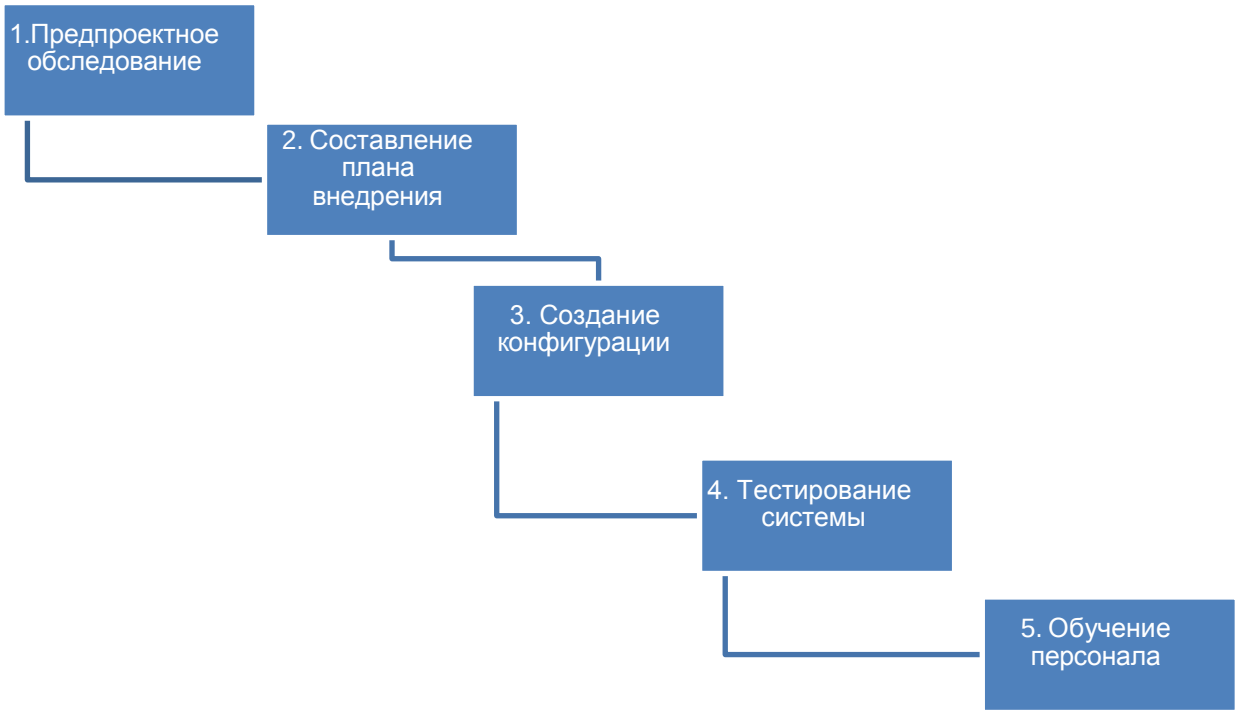

Рисунок 10 – Процессы комплексного этап внедрения

Автоматизация процесса логического тестирования достигается за счет формального характера этих ошибок. Для верификации базы данных в целом и отдельных наборов правил создано большое количество инструментальных средств. Если используемые в процессе вывода цепочки правил небольшие – менее 10, то процесс верификации производят вручную.

Концептуальное тестирование прикладной системы. Работы по внедрению системы выполняются специалистами группы внедрения.

Специалистами внедрения был обработан огромный объем материалов, определена схема информационного взаимодействия системы управления и информационной системы предприятия.

На данном этапе будет разработан проект внедрения системы в среде MS Project. Его скриншоты приведены в приложении Б (Рисунок Б.1 – Б.2).

Модель рисков внедрения комплексной политики информационной безопасности для государственного учреждения "Курганская больница скорой медицинской помощи", включает виды рисков и их влияние на

бизнес-процессы, отображена в таблице 3.11. В данной таблице указаны относительные значения силы риска и вероятности возникновения. Они варьируются в зависимости от конкретной организации и ее информационной инфраструктуры – таблица 16.

Таблица 16 – Модель рисков внедрения проекта

Вид риска	Влияние на бизнес-процессы	Сила риска	Вероятность возникновения
Несанкционированный доступ к медицинской информации	Нарушение конфиденциальности пациентов, возможность утечки медицинских данных	Высокая	Средняя до высокой
Кибератаки и вредоносные программы	Нарушение целостности данных, прерывание работы информационных систем	Средняя до высокой	Средняя до высокой
Физический доступ к информационным ресурсам	Несанкционированный доступ к серверам или хранилищам данных	Средняя	Средняя
Утеря или повреждение данных	Потеря ценной медицинской информации, нарушение континуитета лечения	Средняя до высокой	Средняя
Социальная инженерия	Манипуляция персоналом с целью получения несанкционированного доступа к информации	Средняя	Средняя до высокой
Нарушение требований законодательства о персональных данных	Штрафные санкции, утрата доверия со стороны пациентов	Средняя до высокой	Средняя до высокой
Недостаточная осведомленность и обученность персонала	Возможные ошибки и незнание мер безопасности	Средняя	Средняя до высокой

Выводы по 3 главе

Работа в настоящей диссертации велась по двум практическим направлениям – совершенствование методики по проведению аудита информационной безопасности медицинской организации и разработка решений, направленных на повышение эффективности информационной

безопасности организации.

Предложена методика по проведению аудита информационной безопасности медицинской организации. Преимущество данных методов - высокая точность определения факта атаки. Методика позволяет выявлять не только известные, но и новые типы атак.

В целом на основании анализа предложенной методики, можно утверждать, что предложенная методика является простым и удобным средством моделирования информационно-вычислительных процессов, реализации компьютерных атак и работы программных компонентов в условиях противодействия атакам.

Применение разработанных рекомендаций позволит усовершенствовать исследуемый процесс.

Результатами написания данного раздела магистерской диссертации являются: составление перечня рекомендаций, которые необходимо выполнить в рамках модернизации имеющегося алгоритма проведения проверки эффективности системы информационной безопасности государственного учреждения; определение основных направлений и путей решения имеющихся проблем в области информационной безопасности.

Реализация качественной системы защиты информационных ресурсов сети подразумевает применение комплексных подходов по противодействию попыткам кражи и хищения баз данных. Комплексные подходы подразумевают использование элементов сигнатурного анализа, обнаружения потенциальных опасностей, а также методы функционального анализа. Все это возможно обеспечить за счет применения модернизированного комбинированного способа защиты информационных сетей.

Заключение

В настоящее время информация представляет собой весьма эффективный инструмент, с помощью которого имеется возможность воздействия на экономическую ситуацию. Успешность любого вида деятельности определяется наличием достоверной и защищенной информации. В условиях рыночной экономики наличие исключительных прав пользования той или иной информацией оказывает решающее значение в процессе борьбы за рынок [7].

В настоящее время существует большое число разнообразных методов защиты информации. С их помощью обеспечивается требуемый уровень безопасности и целостности баз данных. Применение тех или иных средств защиты информации определяется степенью подготовки нарушителей. Нарушения информационной безопасности имеет свою классификацию. Они могут быть умышленными и неумышленными.

В настоящее время средства защиты информационных сетей постоянно совершенствуются и развиваются. Это обусловлено тем, что информационные технологии характеризуются высоким темпом развития. На каждую новую разработку мошенников необходимо искать ответные меры тем, кто занимается разработкой систем защиты информации.

В связи с высокой скоростью появления различных инструментов для взлома систем защиты информации не всегда получается найти защитное средство защиты. Это обусловлено следующими факторами:

– постоянное совершенствование и развитие элементной базы, разработка новых программ и приложений, с помощью которых может быть взломана система защиты информации, разработка инструментов взлома криптографических барьеров;

– постоянное усложнение сетевых архитектур, увеличение их быстродействия, рост количества клиентов сетей. Эти факторы способствуют увеличению степени рисков несанкционированного доступа

к информации со стороны третьих лиц;

– в связи с постоянной конкурентной борьбой происходит снижение качества выпускаемых программных продуктов.

Современные условия предъявляют требования к организации процессов управлениям предприятиями различных организационных форм и видов деятельности на основы эффективных принципов, способных поддерживать предприятие на конкурентоспособном уровне. Все разнообразие процессов, происходящих в ходе этого процесса, может быть представлено в виде набора социальных, технических, организационных и экономических проектов.

В процессе выполнения выпускной квалификационной работы получены следующие результаты:

– произведен анализ литературных источников по теме исследования;

– произведен анализ основных понятий информационной безопасности и базовых принципов ее обеспечения для медицинских учреждений;

– проанализировано нормативно-правового обеспечения в области информационной безопасности;

– произведен анализ угроз и уязвимостей медицинских учреждений.

По завершению выполнения работы необходимо отметить, что все поставленные задачи решены, цель научно-исследовательской работы достигнута.

Список используемых источников

1. Алферов, А. П. Основы теории баз данных : учебное пособие / А. П. Алферов, А. Ю. Зубов, А. С. Кузьмин [и др.]. – 2-е изд., испр. и доп. – М.: Гелиос-АРВ, 2017. – 480 с.
2. Ахмад, Д. М., Дубравский, И. Защита от хакеров корпоративных сетей. 2017.
3. Бабенко, Л. К. Современные алгоритмы хеширования и методы их анализа: учебное пособие для студентов вузов, обучающихся по группе специальностей в обл. информ. безопасности / Л. К. Бабенко, Е. А. Ищукова. – М.: Гелиос АРВ, 2018. – 376 с.
4. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (ФСТЭК России).
5. Белов, Е. Б. Основы информационной безопасности. Е. Б. Белов, В. П. Лось, Р. В. Мещеряков, А. А. Шелупанов. – М.: Горячая линия – Телеком, 2019. – 544с.
6. Брассар, Ж. Современная криптология : [пер. с англ.] / Ж. Брассар. – М.: Полимед, 2018. – 176 с.
7. Бова, В. В. Основы проектирования информационных систем и технологий : учебное пособие / В. В. Бова, Ю. А. Кравченко ; Южный федеральный университет, Инженерно-технологическая академия. – Ростов-на- Дону ; Таганрог : Южный федеральный университет, 2018. – 106 с.
8. Бэрмэн, С. Разработка правил информационной безопасности. 2016.
9. Вейцман, В. М. Проектирование информационных систем: Учебное пособие. – М.: МУБИНТ, 2018. – 214 с.
10. Вернер, М. Основы защиты информации : учебник для вузов : [пер. с нем.] / М. Вернер – М. : Техносфера, 2016. – 288 с.
11. Ицик, Б.-Г. Microsoft SQL Server 2012 Основы T-SQL. – М.: Эксмо,

2018. – 401 с.

12. Гвоздева, Т. В. Проектирование информационных систем: технология автоматизированного проектирования. Учебно-справочное пособие / Т. В. Гвоздева, Б.А. Баллод. – СПб.: Лань, 2018. – 156 с.

13. ГОСТ Р ИСО/МЭК 17799-2005. Информационная технология. Практические правила управления информационной безопасностью [Электронный ресурс]. – Введ. 2007–01–01. // СПС Консультант Плюс (дата обращения: 21.04.2023).

14. ГОСТ Р 51275-2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения [Электронный ресурс]. – Введ. 2006–12–27. // СПС Консультант Плюс (дата обращения: 18.03.2023).

15. Гохберг, Г. С. Информационные технологии: Учебник для студ. учрежд. сред. проф. образования / Г. С. Гохберг, А. В. Зафиевский, А. А. Короткин. – М.: ИЦ Академия, 2018. – 208 с.

16. Гудков, П. А. Защита от угроз информационной безопасности: учебное пособие / П. А. Гудков ; под ред. А. М. Бершадского. – Пенза : Изд-во Пенз. гос. ун-та, 2017. – 251 с.

17. Емельянова, Н. З. Проектирование информационных систем: Учебное пособие / Н. З. Емельянова, Т. Л. Партыка, И. И. Попов. – М.: Форум, 2018. – 432 с.

18. Коваленко, В. В. Проектирование информационных систем: Учебное пособие / В. В. Коваленко. – М.: Форум, 2018. – 976 с.

19. Кузнецов, С. Д., Основы баз данных / С. Д. Кузнецов. – М.: Бином. Лаборатория знаний, Интернет-университет информационных технологий, 2018. – 488 с.

20. Методический документ. Методика оценки угроз безопасности информации (утв. ФСТЭК России 05.02.2021).

21. Олифер, В. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов / В. Олифер, Н. Олифер. – М.: СПб Питер,

2016. – 672.

22. Партыка, Т. Л. Информационная безопасность: Учебное пособие / Т. Л. Партыка, И.И. Попов. – М.: Форум, 2018. – 88 с.

23. Перлова, О. Н. Проектирование и разработка информационных систем: Учебник / О. Н. Перлова, О. П. Ляпина, А. В. Гусева. – М.: Academia, 2018. – 416 с.

24. Петренко, С. Д. Основы защиты баз данных в Delphi : учебное пособие / С. Д. Петренко, А. В. Романец, И. С. Лужков [и др.]. – 3-е изд., испр. и доп. – М.: Техносфера, 2017. – 305 с.

25. Пирогов, В. Ю., Информационные системы и базы данных, Организация и проектирование / В. Ю. Пирогов. – М.: БХВ-Петербург, 2019 – 528 с.

26. Проектирование информационных систем: учебник и практикум для СПО / под ред. Д. В. Чистова. – М.: Издательство Юрайт, 2019. – 258 с.

27. Положение о методах и способах защиты информации в информационных системах персональных данных, утвержденное приказом ФСТЭК России от 05 февраля 2010 года № 58 (зарегистрировано Минюстом России 19 февраля 2010 года № 16456).

28. Постановление Правительства РФ «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» от 01.11.2012г. №1119.

29. Приказа ФСТЭК России №21 от 18.02.2013 г. «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

30. Романец, Ю.В., Тимофеев, П. А., Шаньгин, В. Ф. Защита информации в компьютерных системах и сетях. – М.: Радио и связь, 2018.

31. Ростовцев, А. Г. Теоретическая криптография / А. Г. Ростовцев, Е. Б. Маховенко. – СПб.: Профессионал, 2019. – 479 с.

32. Симионов, Ю. Ф., Боромотов, В. В., Информационный менеджмент

/ Ю. Ф. Симионов, В. В. Боромотов. – М.: Феникс, 2018. – 250 с.

33. Симонов, С. В. Методология анализа рисков в информационных системах // Защита информации. Конфидент. 2018. №1. С. 72–76.

34. Склюев, Р. Я. Технологии обеспечения комплексной информационной безопасности в государственном учреждении // Точная наука. – 2022 – № 139. С. 10–12.

35. Стиллмен, Э., Грин, Д. Изучаем C# – СПб.: Питер, 2018. – 816 с.

36. Староверов, Д. Конфликты в сфере безопасности. Социально-психологические аспекты защиты // Системы безопасности связи и телекоммуникаций. – №6. – 2019.

37. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (ред. от 21.12.2013).

38. Федеральный закон Российской Федерации от 26 июля 2006 г. № 149- ФЗ «Об информации, информационных технологиях и о защите информации» (ред. от 28.12.2013).

39. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей: Учебное пособие / В. Ф. Шаньгин. – М.: Форум, 2018. – 256 с.

40. Шпак, В. Ф. Методологические основы обеспечения информационной безопасности объекта // Конфидент. Защита информации. – № 1. – 2017. – С. 75– 86.

41. Шумский, А. А., Системный анализ в защите информации / А. А. Шумский, А. А. Шелупанов. – М.: Гелиос АРВ, 2016. – 224 с.

42. Щеглов, А. Ю. / Защита информации он несанкционированного доступа. – М.: изд-во Гелиос АРВ, 2018. – 384 с.

43. Ярочкин, В. И., Информационная безопасность: учебник для студентов вузов// – М.: Академический проект; Гаудеамус, 2-е изд., 2016 г., 544 с.

44. Being Fluent with Information Technology (2019). Chapter: 1 Why Know About Information Technology? // nap.edu [Электронный ресурс]. – Режим доступа: https://www.nap.edu/read/6482/chapter/3 (дата обращения:

04.05.2023).

45. Coe, N., Harrison, M., Paterson, K. Oxford practice Grammar. Basic: Oxford Unive sity Press, 2019. – 349 p.

46. Definite articles and indefinite articles – determiners in English [Электронный ресурс]. – Режим доступа: http://www.englishlessonsbrighton.co.uk/definite-indefinitearticles-determiners/ (дата обращения: 16.02.2023).

47. Esteras, S. R. Infotech English for computer users. Student's book: Cambridge University Press, 2018. – 172 p.

48. Evans, V., Dooley, J., Wright, S. Information Technology: Express Publishing, 2019. – 122 p.

49. Vince, M. First Certificate Language Practice. English Grammar and Vocabulary: Macmillan, 2018. – 351 p.

Приложение А

Обобщённая модель угроз безопасности

Таблица А.1 – Обобщенная модель угроз безопасности ГБУ «Курганская БСМП»

Наименование угрозы	Вероятность реализации угрозы (Y2)	Возможность реализации угрозы (Y)	Опас-ность угрозы	Актуальность угрозы	Меры по противодействию угрозе	
					Технические	Организационные
1. Угрозы от утечки по техническим каналам						
1.1. Угрозы утечки акустической информации	Y_2=0	Y=0,25	Низкая	Неактуальная		
1.2. Угрозы утечки видовой информации	Y_2=0	Y=0,25	Низкая	Неактуальная		
1.3. Угрозы утечки информации по каналам ПЭМИН	Y_2=0	Y=0,25	Низкая	Неактуальная		
2. Угрозы несанкционированного доступа к информации						
2.1. Угрозы уничтожения, хищения аппаратных средств ИС носителей информации путем физического доступа к элементам ИС						
2.1.1. Кража ПЭВМ	Y_2=0	Y=0,25	Низкая	Неактуальная		
2.1.2. Кража носителей информации	Y_2=0	Y=0,25	Низкая	Неактуальная		
2.1.3. Кража ключей доступа	Y_2=0	Y=0,25	Низкая	Неактуальная		
2.1.4. Кражи, уничтожение информации	Y_2=0	Y=0,25	Низкая	Неактуальная		
2.1.5. Вывод из строя узлов ПЭВМ, каналов связи	Y_2=0	Y=0,25	Низкая	Неактуальная		
2.1.6.Несанкционированное отключение средств защиты	Y_2=0	Y=0,25	Низкая	Неактуальная		
2.2. Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий)						
2.2.1. Действия вредоносных программ (вирусов)	Y_2=5	Y=0,5	Средняя	Неактуальная		
2.2.2. Недекларированные возможности системного ПО и ПО для обработки персональных данных	Y_2=0	Y=0,25	Низкая	Неактуальная		
2.2.3. Установка ПО не связанного со служебным и обязанностями	Y_2=0	Y=0,25	Низкая	Неактуальная		
2.3. Угрозы непреднамеренных действий пользователей и нарушений безопасности функционирования ИС и СЗ в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера						
2.3.1. Утрата ключей и атрибутов доступа	Y_2=2	Y=0,35	Средняя	Неактуальная		
2.3.3. Непреднамеренное отключение средств защиты	Y_2=0	Y=0,25	Низкая	Неактуальная		
2.3.4. Выход из строя аппаратно- программных средств	Y_2=0	Y=0,25	Низкая	Неактуальная		
2.3.5. Сбой системы электроснабжения	Y_2=0	Y=0,25	Низкая	Неактуальная		
2.3.6. Стихийное бедствие	Y_2=0	Y=0,25	Низкая	Неактуальная		

Продолжение Таблицы А.1

2.4. Угрозы преднамеренных действий внутренних нарушителей						
2.4.1. Доступ к информации, модификация, уничтожение лицами недопущенными к ее обработке	Y_2 =0	Y=0,25	Низкая	Неактуальная		
2.4.2. Разглашение информации, модификация, уничтожение сотрудника ми допущенными к ее обработке	Y_2=0	Y=0,25	Низкая	Неактуальная		
2.5. Угрозы несанкционированного доступа по каналам связи						
2.5.1. Угроза «Анализ сетевого трафика» с перехватом передаваемой из ИС и принимаемой из внешних сетей информации						
2.5.1.1. Перехват за переделами контролируемой зоны	Y_2=10	Y=0,75	Высокая	Актуальная	путем использования в составе ИС программных или программно-аппаратных средств (систем) обнаружения вторжений, использующие сигнатурные методы анализа	физическая охрана информационно й системы
2.5.1.2. Перехват в пределах контролируемой зоны внешними нарушителями	Y_2=0	Y=0,25	Низкая	Неактуальная		
2.5.1.3. Перехват в пределах контролируемой зоны внутренними нарушителями.	Y_2=0	Y=0,25	Низкая	Неактуальная		
2.5.2. Угрозы выявления паролей по сети.	Y_2=5	Y=0,5	Средняя	Неактуальная		
2.5.3. Угрозы удаленного запуска приложений.	Y_2=2	Y=0,35	Средняя	Неактуальная		
2.5.4. Угрозы внедрения по сети вредоносных программ.	Y2=10	Y=0,75	Высокая	Актуальная	Должна проводиться автоматическа я проверка на наличие ВПр	физическая охрана информационно й системы

Приложение Б

План проекта внедрения единой политики ИБ

		Начало проекта	24 дней	Пн 17.07.23	Чт
2		**Подготовительный этап**	**16 дней**	**Пт 18.08.23**	**Пт**
3		Предварительный осмотр объекта	2 дней	Пт 18.08.23	Пн
4		Анализ информационной составляющей	3 дней	Вт 22.08.23	Чт
5		Анализ программной и технической составляющей	5 дней	Пт 25.08.23	Чт
6		Изучение планов помещений, схем технических коммуникаций, связи и других документов	4 дней	Пт 01.09.23	Ср
7		Оформление результатов, полученных при проведении осмотра помещений и объектов	2 дней	Чт 07.09.23	Пт
8		**Основной этап**	**5 дней**	**Пн 11.09.23**	**Пт**
9		Подготовка и настройка оборудования	1 день	Пн 11.09.23	Пн
10		Проведение измерений	1 день	Вт 12.09.23	Вт
11		Разработка архитектуры системы ЗИ	1 день	Ср 13.09.23	Ср
12		Формирование списка необходимых технических средств	2 дней	Чт 14.09.23	Пт
13		**Закупка необходимых технических средств**	**4 дней**	**Пн 18.09.23**	**Чт**
14		Анализ рынка, поиск оптимальных поставщиков	3 дней	Пн 18.09.23	Ср
15		Покупка оборудования	1 день	Чт 21.09.23	Чт
16		**Заключительный этап**	**12 дней**	**Пт 22.09.23**	**Пн**
17		Коммутация оборудования	1 день	Пт 22.09.23	Пт
18		Пуско-наладочные работы, проверка функционирования системы	3 дней	Пн 25.09.23	Ср
19		Экономическое обоснование работы	3 дней	Чт 28.09.23	Пт
20		Составление отчетов и рекомендаций	1 день	Пн 09.10.23	Пн

Рисунок Б.1 – План проекта внедрения единой политики ИБ ГБУ «Курганская БСМП»

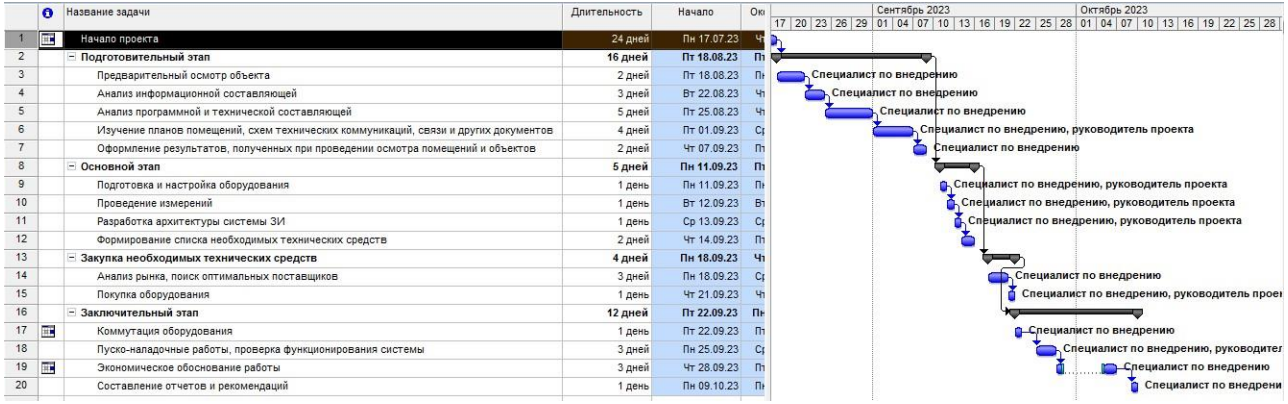

Рисунок Б.2 – Общий вид разработанного проекта