Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
АМУРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
(ФГБОУ ВО «АмГУ»)

Факультет математики и информатики
Кафедра информационных и управляющих систем
Направление подготовки 09.04.04 – Программная инженерия
Направленность (профиль) образовательной программы Управление разработкой программного обеспечения

ДОПУСТИТЬ К ЗАЩИТЕ
Зав. кафедрой
_____ А.В. Бушманов
«_____»_____2021 г.

МАГИСТЕРСКАЯ ДИССЕРТАЦИЯ

на тему: Автоматизированный аудит и контроль информационных активов предприятия

Исполнитель
студент группы 957-ом _____ (подпись, дата) А.А. Ложкова

Руководитель
доцент, канд. техн. наук _____ (подпись, дата) С.Г. Самохвалова

Руководитель
магистерской программы
профессор, док. техн. наук _____ (подпись, дата) И.Е. Ерёмин

Нормоконтроль
инженер кафедры _____ (подпись, дата) В.Н. Адаменко

Рецензент
доцент, канд. техн. наук _____ (подпись, дата) А.Н. Рыбалев

Благовещенск 2021

Министерство науки и высшего образования Российской Федерации

Федеральное государственное бюджетное образовательное учреждение
высшего образования
АМУРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
(ФГБОУ ВО «АмГУ»)

Факультет математики и информатики
Кафедра информационных и управляющих систем

УТВЕРЖДАЮ
Зав.кафедрой
_____А.В.Бушманов
«_____»_____2021 г.

З А Д А Н И Е

К выпускной квалификационной работе студента Ложковой Анны Александровны

1. Тема выпускной квалификационной работы: Автоматизированный аудит и контроль информационных активов предприятия

(утверждено приказом от _____ № _____)

2. Срок сдачи студентом законченной работы 23 июня 2021 г.

3. Исходные данные к выпускной квалификационной работе: предметная область, нормативно-правовая документация, перечень литературы.

4. Содержание выпускной квалификационной работы (перечень подлежащих разработке вопросов): описание предметной области; анализ существующих методов определения и ликвидации угроз информационной безопасности на предприятии; проектирование программного обеспечения; представление результатов фактического тестирования программного обеспечения.

5. Дата выдачи задания 25 февраля 2021 г.

6. Руководитель выпускной квалификационной работы: Самохвалова С.Г., доцент, канд. техн. наук

7. Задание принял к исполнению (_____г.): _____
(подпись студента)

РЕФЕРАТ

Выпускная квалификационная работа содержит 97 страниц, 33 рисунка, 6 таблиц, 59 источников.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ, АВТОМАТИЗИРОВАННЫЙ АУДИТ, ИНФОРМАЦИОННЫЕ АКТИВЫ, КОНФИДЕНЦИАЛЬНАЯ ИНФОРМАЦИЯ, АУДИТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Актуальность темы исследования обусловлена отсутствием комплексного подхода к предотвращению угроз информационной безопасности федеральных органов исполнительной власти и непрерывным ростом объемов обрабатываемой информации в налоговых органах. Кроме того, актуальность выбранной темы обусловлена Приказом Федеральной налоговой службы от 13 января 2012 г. «Об утверждении Концепции информационной безопасности Федеральной налоговой службы».

Цель магистерской работы: разработка и внедрение программного обеспечения для проведения автоматизированного аудита и контроля информационных активов предприятия с целью предотвращения угроз информационной безопасности и совершенствования системы защиты информации.

Разработанное программное обеспечение поможет организациям снизить количество инцидентов информационной безопасности, защитить деятельность организации и противостоять противоправным действиям злоумышленников.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Внедрение новых информационных технологий во всех сферах деятельности человека обуславливает рост значимости информационной безопасности. Нарушения, которые могут быть вызваны несвоевременным выявлением и предотвращением угроз информационной безопасности федеральных органов исполнительной власти, предоставляют угрозу национальной безопасности. Вследствие этого, сфера выявления и противодействия угроз является приоритетной.

Актуальность темы исследования обусловлена отсутствием комплексного подхода к предотвращению угроз информационной безопасности федеральных органов исполнительной власти и непрерывным ростом объемов обрабатываемой информации в налоговых органах. Кроме того, актуальность выбранной темы обусловлена Приказом Федеральной налоговой службы от 13 января 2012 г. «Об утверждении Концепции информационной безопасности Федеральной налоговой службы».

Цель магистерской работы: разработка и внедрение программного обеспечения для проведения автоматизированного аудита и контроля информационных активов предприятия с целью предотвращения угроз информационной безопасности и совершенствования системы защиты информации.

Для достижения поставленной цели были сформулированы следующие задачи:

– рассмотреть основные цели и задачи обеспечения информационной безопасности;

– исследовать нормативно-правовую основу обеспечения информационной безопасности на предприятии;

– проанализировать существующие методы выявления актуальных угроз информационной безопасности на предприятии;

– выявить актуальные угрозы информационной безопасности предприятия;

– разработать полную модель деятельности предприятия;

– выполнить анализ существующих процессов;

– выполнить разработку и внедрение программного обеспечения;

– оценить результаты внедрения.

Объектом данного исследования является информационная безопасность предприятия, а предметом – меры предотвращения угроз информационной безопасности предприятия.

Основные пункты научной/методологической новизны диссертации:

В диссертации проведен анализ литературы и нормативно-справочной документации, по результатам исследования сформированы дополнительные регламенты, которые необходимы для комплексного регулирования информационной безопасности территориальных налоговых органов.

Сформирована таблица перечня угроз с наивысшим уровнем возможной реализации в процессе работы территориальных налоговых органов.

В ходе работы построены модели исследуемых бизнес-процессов и разработан новый метод выявления и предотвращения угроз информационной безопасности.

Практическая значимость исследования:

В рамках магистерской диссертации автоматизированы основные этапы процесса выявления нарушений информационной безопасности. Практическая значимость заключается в:

– усовершенствовании методики предотвращения угроз информационной безопасности в процессе работы территориальных налоговых органов;

– автоматизация основных процессов выявления угроз информационной безопасности.

Основные положения и отдельные результаты работы докладывались и обсуждались в рамках следующих публикаций:

− Самохвалова С. Г., Ложкова А. А. Аудит информационной безопасности на предприятии / С. Г. Самохвалова, А. А. Ложкова // Молодежь XXI века: Шаг в будущее, 2020. – С. 120-121.

− 56 Самохвалова С. Г., Ложкова А. А. Комплексная система защиты информации в организации / С. Г. Самохвалова, А. А. Ложкова // Тенденции развития науки и образования, 2021. – С. 79-82.

− Ложкова А. А. Защита биометрических персональных данных в медицинских информационных системах / А. А. Ложкова // Материалы XIV Международной научной конференции «САМ 2020». – 2020. – С.69-72.

На созданное программное обеспечение получено свидетельство о государственной регистрации программы для ЭВМ от 27.04.2021 г. № 2021616811 «Программа для аудита и контроля рисков информационной безопасности автоматизированных информационных систем».

Эмпирическая база:

При написании магистерской диссертации были приведены результаты собственных исследований, нормативные документы, исследования других авторов по теме исследования, статистические материалы и другие источники.

Магистерская диссертация состоит из введения, четырёх глав, заключения и библиографического списка.

В первой главе диссертации приведены основные сведения об угрозах информационной безопасности, разъясняющие цель, задачи информационной безопасности, классификация угроз информационной безопасности.

Во второй главе осуществлен анализ существующих методов определения и ликвидации угроз информационной безопасности на предприятии. Представлена нормативно–правовая основа обеспечения информационной безопасности и рассмотрены основные методы выявления актуальных угроз информационной безопасности на предприятии.

В третьей главе описаны основные этапы проектирования программного обеспечения. Осуществлен выбор модели жизненного цикла, языка

программирования, а также разработан архитектурный проект и выполнено описание функциональных модулей программного обеспечения.

В четвёртой главе приведены основные результаты фактического тестирования программного обеспечения, представлено подробное описание интерфейса программного обеспечения, функций программного обеспечения.

Приведен анализ достоверности и практической значимости полученного результата.

1 ТЕОРЕТИЧЕСКИЕ АСПЕКТЫ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1.1. Понятие и сущность аудита информационной безопасности

Процесс развития общественных процессов и общества в целом напрямую зависит от качества управления информационными ресурсами. В современном устройстве социальной среды использование информации в вопросах управленческого характера уже не является привилегией исключительно корпоративных структур. На сегодняшний день, информационный ресурс представляет из себя один из наиболее значимых средств для поддержания естественных процессов жизни общества.

Внедрение новых программных технологий, включая алгоритмы обработки информации и усовершенствованные средства связи являются далеко не единственным средством, способствующим развитию вариаций использования информации в обществе. Постоянное изменение восприятия уровня значимости информационных ресурсов среди лиц, создающих и потребляющих данный ресурс, является стимулом к прогрессу развития исследуемой области. На данном этапе развития информационной среды, можно сказать, что информация представляет тот продукт, который определяет условия развития общественных процессов. Этот факт определяет значимость соответствующей реализации концепции информационной безопасности.

Концепция информационной безопасности – это комплексный подход к проблемам обеспечения информационной безопасности, методам и средствам защиты жизненно важных интересов личности, общества, государства в информационной сфере. Концепция служит методологической основой обеспечения информационной безопасности [1].

Концепция информационной безопасности представляет из себя тот документ, значимость которого закреплена и регламентирована на государственном уровне практически всех существующих стран мира. Необходимость предотвращения негативных результатов воздействия на

общественную, политическую и экономическую инфраструктуру обусловлена существованием большого ряда факторов, представляющих угрозы для нормального процесса развития информационной среды. Несмотря на регулирование этого вопроса на законодательном уровне, этимология, определяющая рамки информационной безопасности, не имеет достаточно конкретной трактовки.

Отсутствие определенного представления об информационной безопасности в целом, политики ее проведения и границ ее реализации может стать причиной неэффективного выбора мер по обеспечению необходимого уровня защиты информационных ресурсов от возможных угроз.

Сущность информационной безопасности в широком понимании заключается в выявлении и устранении негативных источников воздействия на информацию. Методы и цели защиты информационного ресурса также могут определять ее сущность. Исходя из этого, можно полагать, что реализация комплексного обеспечения информационной безопасности отожествляется с самим определением защиты информации. Многие специалисты определяют сущность информационной безопасности как отсутствие какой–либо возможности источнику угрозы оказать негативное воздействие на объект защиты информации, которое может нанести ущерб его функциональной деятельности или самим свойствам объекта защиты [2].

Официальное определение информационной безопасности представлено в Доктрине информационной безопасности от 05.12.2016. Для более наглядного представления об основных составляющих официального определения информационной безопасности представлена системообразующая схема на рисунке 1.

Рисунок 1 – Основные составляющие определения информационной безопасности

Сформированное в Доктрине информационной безопасности определение выделяет конкретный перечень объектов, обеспечение информационной безопасности которых, необходимо реализовать, а также перечисляет условия, которыми следует руководствоваться при осуществлении политики информационной безопасности [4]. Эта информация представляет сформированную концепцию по руководству и регулированию обеспечения информационной безопасности государства.

Прежде всего, необходимо обратить внимание на отсутствие конкретно сформированного и изложенного значения, которое вкладывается в понятие защищенность. Рассматриваемое понятие защищенности может предполагать как отсутствие возможности воздействия угроз на объекты защиты или соответствующий уровень функционирования системы защиты информации, который способен обеспечить отсутствие угроз, так и непосредственно сам

факт отсутствия угроз. В качестве объектов защиты не совсем корректно рассматривать помимо интересов личности и общества, государственные интересы, поскольку они не могут являться субъектами права. Кроме того, эти понятия несут разно сущностный характер и недостаточно конкретны по определению.

Органы власти и частные предприятия, как правило, обеспечивают свою работу такими системами защиты информации, характеристики которых не могут обеспечить информационную безопасность в полноценной размере, так как, исходя из изложенного в Доктрине информационной безопасности определения, состояние защищенности относится к наиболее значимым сторонам государственного управления и жизни общества. В подобном определении прослеживается отклонение от существующей сути информационной безопасности, так как предметом регулирования становится формировании общественных отношений, что само по себе, представляет новый подход к определению состояния защищенности.

Необходимо отметить, что сама характеристика состояния защищенности по отношению к объекту в области информационной безопасности не может быть классифицирована как способ контроля каждой единицы хранимой и обрабатываемой информации на каждом устройстве с учетом любой возможности негативного воздействия. Обеспечить подобное устройство системы защиты информации представляется крайне сложным и чрезмерно материально затратным даже для представителей некоторых структур государственной власти, не учитывая при этом большую часть общественных интересов. Именно эффективная защищенность общества является наиболее значимым фактором в системе информационной безопасности и реализация мер в данном вопросе должна быть соразмерна действительному уровню общественных затрат. Это является обоснованием для формирования более уточняющего определения, которое бы предполагало под защищенностью реализацию мер, направленных на предотвращение ущерба критической

инфраструктуре и создание условий для поддержания всех сфер деятельности общества.

Процесс формирования условий для эффективного развития общества является неотъемлемой составляющей функционирования информации в социальной среде. Эксплуатация концепции информационной безопасности с учетом средств защиты информационной безопасности влечет за собой определенные ограничения, связанные со свободным использованием информационного ресурса, а создание условий для общественного развития предполагает отсутствие пассивных угроз. Например, развитие платформ для мобильных устройств представляет общественный интерес, но ограничение возможных действий сторонними пользователями в рамках этих платформ может представлять пассивную угрозу информационной безопасности. В данном случае наиболее эффективным методом противодействия угроз будет являться не устранение возможной угрозы, а развитие программного обеспечения на уровне страны, которое обеспечит соответствующий уровень обслуживания социальных потребностей в сфере передачи данных.

Учитывая специфику общественных интересов области информационной безопасности, было бы эффективнее ранжировать способы реализации обеспечения безопасности по приоритетам. К безопасности персональных данных, в сою очередь, можно отнести безопасность личной информации, тогда определение критической инфраструктуры следует расширить до критических интересов. Исходя из вышесказанного, следует понимать, что защита персональных данных обоснованно следует отожествлять с защитой конфиденциальной информации и представлять из себя социальную ценность. В данном ключе, информационная безопасность реализуется по большей мере путем предупреждения несанкционированного доступа к информации. В дополнение, анализ объектов защиты демонстрирует недостаточную оценку значимости такого объекта защиты, как нормальные условия использования информационной безопасности, которые при условии стабильной реализации могли бы значительно сократить негативные воздействия на объекты защиты.

Необходимо отметить, что развитие общественных процессов предполагает развитие культуры страны. Поэтому сфера пассивной защиты информационных ресурсов должна предполагать интересы свободы обращения информации всех отраслей, не находящихся на уровне критической значимости. Критические интересы, в свою очередь, определяют использование именно административных и технических методов обеспечения информационной безопасности, которые в отличие от интересов, не представляющих критической значимости, взаимосвязаны с определенными ограничениями и запретами.

Область социального развития в большей степени предполагает приоритет направления политики дозволения, который включает финансовую поддержку развития области информационной безопасности со стороны общества. Рассматривая механизм обеспечения информационной безопасности, можно отметить недостаточный перечень полномочий региональной и муниципальной власти в области развития и обеспечения информационной безопасности на уровне региона и определенного муниципалитета, в частности. Данные уровни власти могут обеспечить более рациональное устройство развития общества и реализовать механизмы пассивной защиты, несущие профилактический характер обеспечения информационной безопасности общества.

Исходя из вышесказанного, можно сделать вывод, что сущность информационной безопасности включает процессы разработки и реализации активной защиты по отношению к интересам, имеющим критический уровень значимости, а также реализацию пассивной защиты, предполагающая формирование условий для нормального развития общественных процессов и экономической отрасли. Анализ показал, что в данных областях имеет место вариативность способов и средств достижения эффективного обеспечения защищенности информационных ресурсов.

По отношению к экономическому и общественному развитию задействована политика дозволения, а также преимущественно преобладают средства, поощряющие развитие экономики и общества с позиции информационной безопасности. В отношении критических интересов, представляющих наибольший приоритет в активной защите, в основном задействованы административные методы и преобладает использование средств технической защиты информационных данных.

Таким образом, сущность информационной безопасности – это такое состояние объекта, при котором состояние информационной среды, в которой он находится, обеспечивает ему сохранность возможности и способности принимать и реализовывать решения соответственно своим целям, направленным на прогрессивное развитие [5].

1.2 Цели и задачи обеспечения информационной безопасности

Главной целью обеспечения информационной безопасности является защита субъектов информационных взаимоотношений от ущерба, который может нести моральный или материальных характер. Ущерб может быть осуществлен путем намеренного или непреднамеренного получения доступа к информационным ресурсам или вмешательства в процесс работы автоматизированной системы.

В общем смысле можно выделить три основных направления для достижения данной цели: постоянное обеспечение конфиденциальности защищенной информации, обеспечение доступности информации пользователям информационной системы и сохранение целостности циркулируемой в организации информации.

Стратегической целью обеспечения информационной безопасности является содействие и укрепление процесса развития системы обеспечения информационной безопасности.

Обеспечение информационной безопасности должно осуществляться с учетом установленных, общих принципов, поскольку информационная безопасность является связующим элементом реализации информационной и

национальной политики. Основные задачи в области обеспечения информационной безопасности на уровне государственного регулирования [6]:

– формирование единой концепции государственной политики по обеспечению конституционных прав граждан на информационную деятельность;

– модернизация действующего законодательства в соответствии с внедрениями новых технологий в сфере информационной безопасности;

– определение границ полномочий и координация деятельности органов государственной власти Российской Федерации в области информационной безопасности;

– создание соответствующих условий для высокой степени защиты информационных ресурсов федеральных и государственных органов власти;

– поддержка развития отечественных разработок в области информационных технологий;

– поддержка развития информационных и телекоммуникационных средств связи и систем;

– разработка методов и критериев определения уровня информационной безопасности Российской Федерации.

Выявленные задачи обеспечения информационной безопасности относятся к регулированию взаимоотношений в рамках информационного среды со стороны государства. Тем не менее, тема защиты информации на локальном предприятии также очень востребована на данный момент, поскольку действия неправомерного характера, такие как: получение несанкционированного доступа, искажение или уничтожение конфиденциальных данных может повлечь за собой значительный материальный ущерб компании.

Задачи обеспечения информационной безопасности на предприятии могут различаться в зависимости от сферы деятельности и уровня технической оснащенности той или иной компании. Очевидно, что задачи предприятия

более узконаправленны, чем задачи государства. Несмотря на это, можно также выделить общие характеристики задач:

– своевременное прогнозирование, выявление или устранение угроз информационной безопасности;

– разработка и реализация эффективной системы по выявлению уязвимостей и своевременному реагированию на них;

– внедрение средств обеспечения информационной безопасности, нормативно–правового и технического характера;

– сокращение возможных угроз путем регулярной профилактической деятельности.

В рамках магистерской диссертации реализовано исследование целей и задач обеспечения информационной безопасности в ФНС России.

В соответствии с целями обеспечения информационной безопасности ФНС России, изложенных в Приказе ФНС России «Об утверждении Концепции информационной безопасности Федеральной налоговой службы» в перечень которых входят такие виды деятельности, как:

– противодействие негативному информационному воздействию на информацию;

– предотвращение нарушений конституционных прав субъектов в процессе обработки информации;

– предотвращение несанкционированного доступа к конфиденциальной информации;

– предотвращение возможных нарушений в порядке и процессе доступа к информации.

Основные задачи обеспечения информационной безопасности ФНС России:

– анализ реализации возможных угроз и ущерба, создание условий для предотвращения последствий нарушения в системе информационной безопасности;

– своевременная модернизация нормативно-правовой базы, регламентирующей деятельность ФНС России в области защиты информации;

– предотвращение возможности несанкционированного доступа в функционирование информационной системы Федеральной налоговой службы;

– своевременное внедрение средств защиты информации для обеспечения защищенности информационной системы;

– постоянный контроль выполнения всех действий пользователей информационной системы с целью обеспечения информационной безопасности.

Предотвращение и (или) минимизация ущерба субъектам правоотношений в результате противоправных действий со стороны злоумышленников, таких как разглашение, утрата, утечка, модификация, а также обеспечение бесперебойной работы телекоммуникационной инфраструктуры ФНС России, используемой для информационного обмена и взаимодействия с органами государственной власти и организациями является главной целью в рамках обеспечения информационной безопасности в ФНС России.

Основными целями обеспечения безопасности информации являются:

– предотвращение несанкционированного доступа к информации ограниченного доступа;

– предотвращение нарушений прав субъектов при обработке конфиденциальной информации;

– недопущение воздействия на технические средства обработки информации;

– недопущение разрушительного информационного воздействия на информационные активы.

Основными задачами, вытекающими из целей обеспечения безопасности информации в ФНС России, являются:

– совершенствование политики ФНС России в области информационной безопасности;

– соответствие мер и средств защиты информации в информационных системах положениям организационно-распорядительным документам в сфере обеспечения информационной безопасности;

– совершенствование нормативно-правовой базы обеспечения информационной безопасности;

– обеспечение полноты, достоверности и оперативности получения информации налогоплательщиками и органами государственной власти в рамках организации межведомственного взаимодействия;

– защита от вмешательства в процесс функционирования информационных систем посторонних лиц,

– усовершенствование средств защиты информации для предотвращения и нейтрализации угроз информационной безопасности;

– предотвращение несанкционированных действий и незаконных посягательств на информационные активы налоговых органов ФНС России со стороны злоумышленников, посторонних лиц и сотрудников ФНС России, не обладающих разрешающими функциями в рамках должностной инструкции;

– регистрация событий, которые могут повлиять на полноценное и постоянное функционирование информационных систем;

– своевременное выявление источников угроз, причин и условий, способствующих нанесению ущерба, нормального функционирования и развития информационных систем;

– обеспечение возможности резервного восстановления информационных систем при нарушении информационной безопасности.

Своевременное определение актуальных задач на предприятии способствует не только сокращению материальных затрат, но и предотвращению возможных нарушений информационной безопасности.

1.3 Классификация угроз информационной безопасности

Информационная среда является системообразующим звеном в естественном функционировании общественных процессов. Она обеспечивает процессы потребления, хранения и преобразования информации.

Информационная безопасность играет ключевую роль в эффективной и надежной работе предприятия любой сферы деятельности. Этот факт способствует пристальному вниманию многих специалистов к проблематике информационной безопасности.

С учетом активного развития информационных технологий, появления интернета вещей и нарастающего темпа роста всемирной глобализации для руководителей предприятий открывается новый ряд способов использования информации для более эффективной и рациональной оптимизации рабочего или производственного процесса. Эффективное использование информации положительно влияет не только на внешнюю коммуникацию компании, но и на внутреннюю. Для оценки объективности принятия тех или иных решений и повышения показателей производительности многие предприятия используют в своей работе автоматизированные системы обработки информации. Это позволяет значительно повысить продуктивность процессов и сэкономить временные затраты, что, в конечном счете увеличивает прибыль предприятия. Подобные системы имеют большое количество уязвимостей и обеспечение безопасности в данном случае становится вопросом первостепенной важности.

Стоит отметить, что с учетом увеличения количества информационных потоков и разновидностей их использования, уровень угроз информационной безопасности значительно возрастает [7]. Именно поэтому необходимо выявить весь перечень возможных нарушений системы, которые могут представлять опасность и выявить наиболее актуальные виды угроз уже на этапе создания системы информационной безопасности.

Прежде, чем классифицировать возможные виды угроз информационной безопасности, необходимо подробно рассмотреть существующую этимологию данного словосочетания. Угроза информационной безопасности – это совокупность условий и факторов, создающих опасность нарушения информационной безопасности. Стратегия национальной безопасности дает общее определение понятия «угрозы» и рассматривает их как «прямую или косвенную возможность нанесения ущерба конституциональным правам,

свободам, достойному качеству и уровню жизни граждан, суверенитету и территориальной целостности, устойчивому развитию Российской Федерации, обороне и безопасности государства». В отличие от правового акта, регламентирующего основные положения национальной безопасности, толковый словарь им. С.И. Ожегова не затрагивает вопросы национального значения и определяет угрозу как возможную, еще не реализованную опасность. В данном случае под угрозой предполагается опасность наступления изменений, а не сам процесс.

Таким образом, в процессе исследования проблем, связанных с информационной безопасностью необходимо учитывать не только фактическую, но и потенциальную угрозу причинения ущерба. Под термином «информационная безопасность» общепринято подразумевать защищенность информационной системы от преднамеренного и случайного вмешательства, которое может нанести ущерб пользователям информации либо ее владельцам.

Угроза информационной безопасности – это совокупность факторов и последствий, которые могут создать потенциальную или фактическую опасность личности, общества и государства. Такими факторами может быть весь перечень основных принципов функционирования Интернета. Среди них: принципы иерархичности, демократичности, децентрализации, конвергенции и экстерриториальности. В общем смысле под угрозами информационной безопасности принято понимать совокупность факторов и условий, которые создают опасность нарушения безопасности и целостности информации, в том числе копирование, распространение, изменение, блокирование, несанкционированный доступ или иные неуполномоченные действия с защищенной информацией.

Для реализации угроз информационной безопасности необходимо создание канала между носителем информации и источником угрозы, что создает благоприятную среду для нарушения безопасности информационной системы. Существуют три основных элемента для реализации угроз информационной безопасности, это: источник информации, среда

воздействия и носитель. Источником угроз информационной безопасности может выступать материальный объект, субъект или определенное физическое явление, несущее угрозу. Среда воздействия информации представляет собой тот путь распространения информации, в котором определенные программы, данные или сигнал могут оказывать воздействия на доступность, целостность и конфиденциальность защищенной информации. Роль носителя информации может играть как материальный предмет или физическое лицо, так и информационное поле.

Анализ отрицательных воздействий осуществления и возникновения угроз включает в себя обязательную идентификацию возможных источников уязвимостей, угроз, а также методов их реализации. Для осуществления эффективной и комплексной идентификации и дальнейшего устранения потенциальных угроз информационной безопасности необходимо выстроить четкую классификацию.

Общая классификация угроз информационной безопасности осуществляется [8,9]:

- по источнику угроз информационной безопасности;
- по степени вероятности осуществления;
- по объекту воздействия;
- по способу реализации;
- по положению источника;
- по характеру источника;
- по последствиям.

Рассмотрим перечисленные категории более детально. Источники угроз информационной безопасности можно разделить на три группы: антропогенные, технические и природные, но для более подробной классификации необходимо проанализировать каждую из них. Классификация по источнику угроз информационной безопасности представлена на рисунке 2.

Рисунок 2 – Классификация по источнику угроз информационной безопасности

К группе антропогенных угроз относятся субъекты, которые имеют санкционированный или несанкционированный доступ к информации. Антропогенные источники, в свою очередь, также можно разделить на внутренние и внешние. И внешние, и внутренние антропогенные источники угроз информационной безопасности могут быть преднамеренными или случайными.

К непреднамеренным внутренним источником антропогенного характера угроз можно отнести персонал, некорректные действия которого могут представлять угрозу информационной безопасности. Подобного рода угрозы возникают, как правило, из-за ошибок программного обеспечения, отказов, сбоев или повреждений информационной системы.

Внутренние антропогенные источники составляют группу штатных сотрудников предприятия. Особое значение в данной категории угроз занимают случайные нарушения сотрудниками требований эксплуатации техники или некорректное использование информации. Такую группу представляет основной, технический и вспомогательный персонал. К ним могут также

относится и высококвалифицированные специалисты, работающих в сфере эксплуатации технических средств и программного обеспечения [8].

Преднамеренные источники угроз отличаются именно умышленной дезорганизацией работы. Искажение, кража, взлом информации осуществляется путем несанкционированного доступа в конфиденциальные информационные ресурсы.

Особое внимание следует уделить именно преднамеренным угрозам, как от внутренних, так и от внешних источников угроз информационной безопасности антропогенного характера. Реализация угрозы и осуществление несанкционированного доступа может протекать путем: элементов информационной инфраструктуры, которые могут оказаться вне контроля из–за сопутствующих процессов, таких как: ремонт, сопровождение или утилизация; использования вредоносных программ, программных или алгоритмических закладок; несанкционированного подключения к каналам связи, которые выходят за территориальные пределы предприятия; использования автоматизированных рабочих мест, которые подключены к сетям общего пользования. Также необходимо учитывать, что группу внутренних источников могут составлять специально обученные агенты или люди с нарушениями психики.

Стоит отметить, что угрозы, расположенные за пределами контролируемой предприятием зоны или внешние угрозы в системе информационной безопасности, не обязательно несут преднамеренный характер. В зависимости от особенностей организации информационной и технической системы предприятия определенные действия внешних субъектов могут повлечь отклонения основных критериев информационной безопасности. Это может осуществиться в процессе стандартной эксплуатации системы с использованием доступа внешних интерфейсов. К внешним антропогенным источникам можно отнести: конкурирующие организации, партнеров, структуры криминального характера, силовые структуры,

провайдеров услуг связи, потенциальных злоумышленников и пользователей информационной системы.

Техногенные источники угроз информационной безопасности также могут подразделяться на внутренние и внешние, и зависят исключительно от технической составляющей. Роль внешних техногенных источников угроз обычно выполняют сети коммуникаций и средства связи: канализация, водоснабжение, отопление, линии передач данных, телефонные линии и прочее.

Внутренние техногенные источники угроз информационной безопасности могут проявляться в некачественных программных средствах обработки информации, вредоносных программах и аппаратных закладках.

Природные источники угроз информационной безопасности отличаются своей непредсказуемостью и могут иметь исключительно внешний характер. К ним относятся такие стихийные бедствия, как: пожары, ураганы, землетрясения и наводнения. Стоит добавить, что данный вид информационной угрозы меньше предыдущих поддается прогнозу и противодействию. Однако, многие предприятия обеспечивают своих сотрудников четкой инструкцией на случай возникновения чрезвычайной ситуацией, которая помогает сократить ущерб.

Все источники угроз имеют разный уровень вероятности, который можно рассчитать с учетом косвенных показателей, таких как: возможность возникновения, готовность источника и фатальность.

Классификация угроз информационной безопасности по объекту воздействия содержит угрозы нарушения безопасности информации, которые могут быть реализованы путем воздействия на серверы, взаимодействие каналов связи, использования автоматизированных рабочих мест и определенных средствах обработки информации, таких как принтеры, мониторы и проекторах.

Реализация угрозы информационной безопасности направлена на нарушение процесса эксплуатации информационной системы, а также может

направлена на главные свойства информации: доступность, актуальность, целостность и конфиденциальность.

Классификация по способу реализации угрозы информационной безопасности состоит из следующих видов [9,10]:

– намеренное воздействие на информационную систему предприятия с использованием уязвимостей аппаратного и программного обеспечения или вирусных программ;

– утечка информации техногенного характера;

– социальная инженерия, то есть использования методов воздействия непосредственно на человека с целью несанкционированного доступа к информационным ресурсам.

По положению источника можно выделить два вида угроз:

– источник угрозы расположен в пределах контролируемой предприятием зоны;

– источник угрозы расположен за пределами контролируемой предприятием зоны.

– По характеру можно также выделить два вида угроз:

– пассивные угрозы, которые не оказывают влияния на работу информационной системы, но могут нарушить определенные правила границ доступа к сетевым ресурсам или прочей информации;

– активные угрозы, которые оказывают непосредственное воздействие на информационную систему, нарушая границы доступа к сетевым ресурсам и информации.

Также угрозы информационной безопасности можно классифицировать по следующим основным критериям:

– способ осуществления угрозы. Выделяют преднамеренные, случайные действия, а также чрезвычайные ситуации техногенного или природного характера;

− нацеленность угрозы на важнейшие свойства информации такие как: конфиденциальность, целостность, доступность. Именно против этих составляющих в первую очередь направлены информационные атаки;

− компоненты информационных технологий и систем. На что непосредственно нацелены угрозы: сети, данные, программно-аппаратные комплексы, иная поддерживающая инфраструктура, а также аппаратная часть информационной системы;

− локализация источника угрозы. Она может быть, как внутри информационной системы, так и вне системы или технологии.

Для дальнейшего исследования необходимо проанализировать основы классификации угроз информационной безопасности систем удаленной обработки данных, поскольку выбранный объект исследования задействует этот процесс в своей работе. В процессе удаленной обработки данных разного характера задействованы информационно-измерительные системы, которые, в свою очередь, состоят из трех основных структурных составляющих, а именно: программная, коммуникационная и аппаратная.

Следовательно, среди угроз, направленных на нарушение безопасности информации, можно также выделить [11]:

− угрозы, которые связаны непосредственно с аппаратной частью информационной системы;

− угрозы, которые связаны с коммуникационной системой;

− угрозы, характерные для программного обеспечения.

Наглядную схему классификации вышеперечисленных угроз можно рассмотреть более подробно на рисунке 3.

Рассмотрим более детально класс угроз, который характерен для программного обеспечения информационной системы предприятия. Угрозы данного кластера направлены на информацию, хранящуюся в памяти. Процесс записи данных за или перед пределами выделенного буфера программой, затирая тем самым данные называется переполнение буфера.

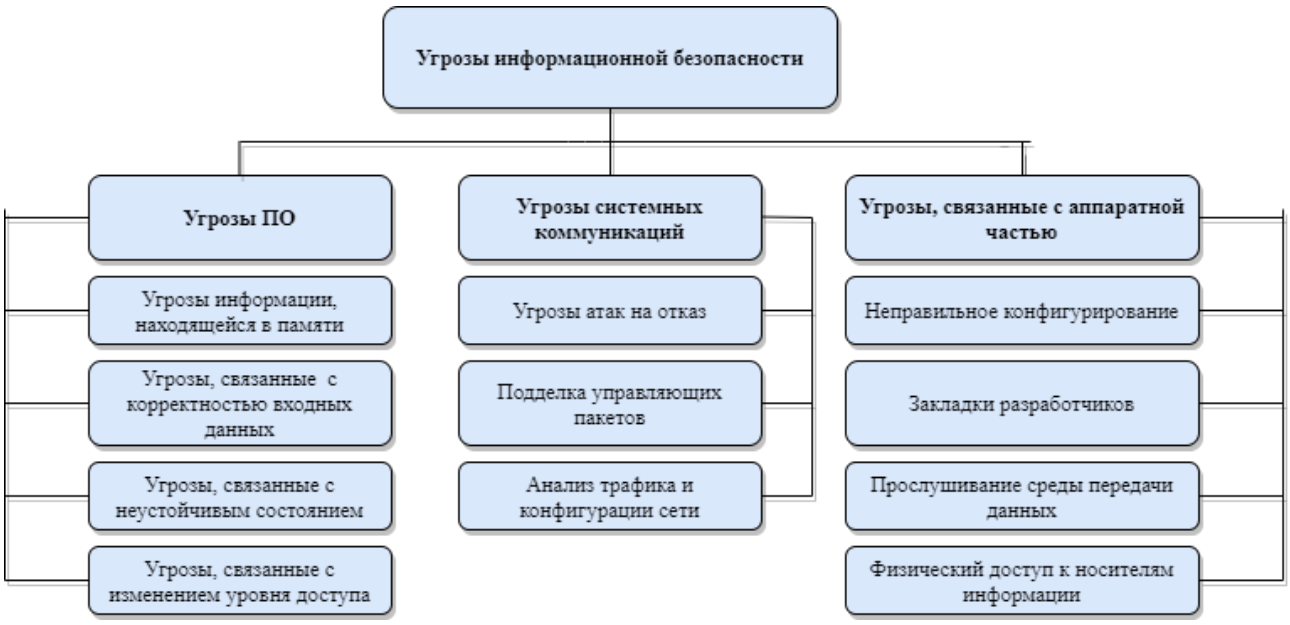

Рисунок 3 – Классификация угроз информационной безопасности в информационных системах

Это явление является причиной нарушения конфиденциальности, доступности и целостности информации. Подобную ситуацию может спровоцировать неправильная работа с данными.

Также, к угрозам, направленным на информацию, хранящуюся в памяти, можно отнести вредоносную ссылку на объект, с помощью которой злоумышленник получает несанкционированный доступ к информации, хранящейся на определенном участке памяти. В эту же группу можно отнести угрозы, которые связаны с некорректностью входных данных и изменением уровня доступа.

Угроза внедрения в запросы также является видом угроз, направленным на информацию, хранящуюся в памяти. Этот метод основан на внедрении в запрос произвольных команд, что может спровоцировать нарушение целостности и конфиденциальности информации.

Незащищенный доступ к областям информационной системы позволяет пользователю открыть доступ к областям системы, играющим принципиально значимую роль в работоспособности системы.

Рассмотрим угрозы, которые характерны для системы коммуникаций. К этой группе угроз можно отнести различные виды информационных атак в сети Интернет. Среди этих атак можно выявить следующие:

- простая атака на отказ. Принцип действия данной атаки заключается в превышении отправляемых запросов системе, что в последствии, приводит к неспособности системы обработать запрашиваемое количество информации и, в конечном счете, система ограничивает доступность информации;
- распределенная атака на отказ. В отличие от простой атаки на отказ, распределенная атака задействует большое количество рабочих станций;
- подделка пакетов управляющих сетевых устройств;
- перехват сетевого трафика;
- сканирование. Получение доступа к сетевым портам информационной системы с целью выявления уязвимостей программного обеспечения.

Последняя группа угроз относится к аппаратной части. К этой группе можно отнести следующие виды угроз:

- неправильная конфигурация аппаратных средств. Некорректная настройка аппаратной части может стать причиной физического повреждения или отказа работы аппаратуры;
- получение физического доступа к носителю информации;
- использование закладок. Несанкционированное использование злоумышленниками закладок может привести к нарушению конфиденциальности, целостности и доступности информации. Этот вид угрозы характерен для аппаратных устройств без использования процесса аутентификации;
- аппаратное прослушивание данных. Подразумевается перехват сообщений, путем использования беспроводной сети или физическое подключение злоумышленника к средству передачи данных. Этот вид угрозы характерен для распределительных систем с низким уровнем криптостойкости.

Таким образом, можно утверждать, что классификация угроз информационной безопасности может быть проведена по множеству различных показателей. Наиболее распространенным показателем в отечественной и зарубежной научно-публицистической литературе является показатель природы возникновения угрозы, именно этот показатель был проанализирован максимально детально.

Следует отметить, что наиболее распространены непреднамеренные ошибки и именно они представляют из себя наибольшую опасность и наибольшую возможность причинения ущерба. Чаще всего, эти ошибки и являются угрозами, но также они могут являться причинами возникновения угроз, создавая уязвимые места в информационной системе. К таким ошибкам можно отнести непреднамеренные действия, некорректно введенные данные системных администраторов, операторов, штатных пользователей или иных лиц, занимающихся обслуживанием информационной системы. Пользователи системы могут являться источниками таких угроз, как: непреднамеренное или намеренное искажение или ликвидирование данных, техническое отсутствие возможности работы с информационной системой, отсутствие соответствующей подготовки пользователя, что, в свою очередь может спровоцировать некорректное использование информации.

Наиболее эффективным способом устранения ошибок непреднамеренного характера является строгий регламент любых действий пользователей, а также максимальная стандартизация и автоматизация процессов.

2 АНАЛИЗ СУЩЕСТВУЮЩИХ МЕТОДОВ ОПРЕДЕЛЕНИЯ И ЛИКВИДАЦИИ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ПРЕДПРИЯТИИ

2.1 Нормативно–правовая основа обеспечения информационной безопасности

Информационное общество представляет из себя целую систему по производству, переработке и хранению информации. Наличие нормативно–правовой базы, регулирующей взаимоотношения субъектов в сфере информационных отношений, является обязательным условием для нормальной жизни общества. С помощью правовой базы, соответствующей актуальным проблемам и тенденциям информационного характера, становится возможным предотвратить угрозу или защитить свои права на тот или иной вид информации. Правовое регулирование принимает принципиально важное значение в сфере безопасности федеральной и государственной службы, включающей гражданскую, военную и правоохранительную. Необходимо проанализировать вопрос актуальности нормативно-правовой базы обеспечения информационной безопасности с целью выявления сильных и слабых сторон защиты прав граждан на территории Российской Федерации.

Существование правовой базы для урегулирования вопросов взаимоотношений в сфере информации подразумевает наличие отдельной группы нормативно–правовых актов, которые регулируют сферу информационной безопасности. На территории Российской Федерации действует следующий перечень основных нормативно-правовых актов и Федеральных Законов:

- Конституция РФ;
- Гражданский Кодекс Российской Федерации;
- Уголовный Кодекс Российской Федерации;
- Доктрина информационной безопасности;
- ФЗ № 128 – «О лицензировании отдельных видов деятельности»;

– ФЗ № 149 – «Об информации, информационных технологиях и защите информации»;

– ФЗ № 152 – «О персональных данных».

Нормативно-правовая база, определяющая и регулирующая основные положения информационной безопасности, находится в процессе постоянного, не прекращаемого обновления. Усовершенствования правовой базы происходят ежегодно. Это необходимо для поддержания актуальности юридической базы и для своевременного соответствие развивающихся технологий с отраслью права. Развитие новых возможных правоотношений в области информационной безопасности также является причиной постоянной модернизации правового регулирования.

Учитывая большой перечень федеральных законов, нормативно–правовых актов и других разноплановых по своему характеру юридических документов, можно отметить, что отрасль информационной безопасности требует больших затрат для реализации полноценного регулирования со стороны государственной власти. Что также подтверждает необходимость частого и комплексного пересмотра текущей правовой структуры.

В Конституции РФ закреплены исходные положения обеспечения безопасности. Определение безопасности в основном законе встречается в одиннадцати статьях. При этом, стоит учитывать, что «безопасность» относиться как к личности и обществу, так и к государству. Конституция РФ определяют различные виды безопасности. В статьях 13, 55, 82 и 114 вводится определение государственной безопасности. В тексте документа выделены экологические, общественные виды безопасности, а также безопасность граждан.

В Конституции РФ наиболее частым по упоминанию термином, связанным с видами безопасностью, является «безопасность личности». Данный вид безопасности подразумевает защищенность прав и свобод человека и гражданина, включая права на информационную безопасность [12].

Это утверждение является основополагающей составляющей

безопасности страны.

На данном этапе развития правового регулирования информационной безопасности наиболее приоритетным вопросом становится своевременность разрабатываемых предложений по эффективной защите прав человека в области информационного пространства.

Прогрессирующее развитие информационной среды оказывает воздействие на важнейшие отрасли безопасности страны, такие как: военная, экономическая и политическая. Стоит отметить, национальная безопасность страны зависит от уровня информационной защищенности и качественной реализации обеспечения информационной безопасности.

Доктрина информационной безопасности также является основополагающим документов в вопросах безопасности государственного и личного характера. Содержание Доктрины включает информацию о том, что права граждан на неприкосновенность частной жизни и информации не имеют необходимого уровня технического и правого обеспечения на момент публикации документа. Недостаточный же уровень организации системы защиты и у федеральных органов государственной власти, государственных органов власти и органов местного самоуправления. Нарушения обеспечения информационной безопасности вышеперечисленных органов могут повлечь за собой череду тяжелых последствий, поскольку процесс работы органов напрямую связан с накоплением и хранением огромного количества персональных данных [13].

Кодекс административных правонарушений также имеет область регулирования, затрагивающую сферу информационной безопасности. В основном она затрагивает правонарушения, которые связаны со средствами массовой информации.

Текущее положение обостряется с течением времени и появлением большего «InfoWatch» к концу 2020 года по всему миру в открытом доступе оказалось вдвое больше пользовательских данных, чем в предыдущем. На территории Российской Федерации рост утечек увеличился более чем на 40%.

Основываясь на ведомственных статистических данных о состоянии судимости на 2020 год судебного департамента при Верховном Суде России, количество осужденных по ст.137 «Нарушение неприкосновенности частной жизни» Уголовного кодекса Российской Федерации составляет 171 человек, в 2018 году – 127, в 2017 году число осужденных составляло 86 человек. Динамику роста преступлений, связанных с нарушением неприкосновенности частной жизни можно рассмотреть более наглядно на рисунке 4.

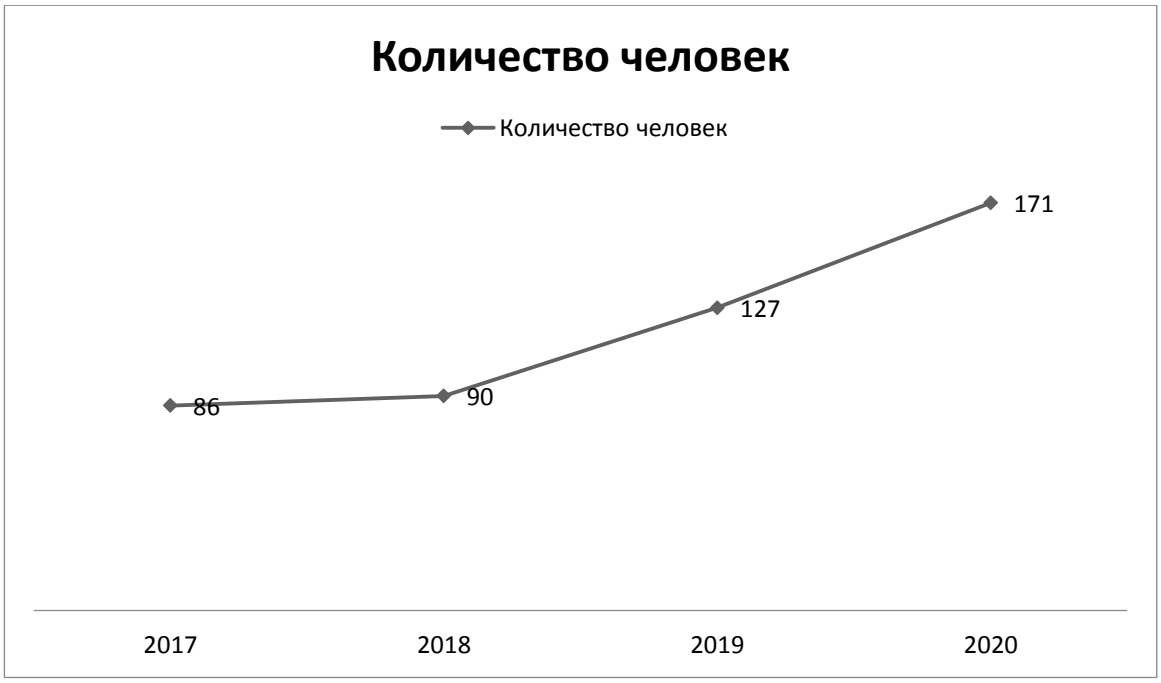

Рисунок 4 – Динамика числа осужденных по ст.137 УК РФ

Осуждение по этой статье предполагает незаконное распространение или собирание информации. Показатели количества осужденных по другим статьям, связанным с нарушениями информационной безопасности, также имеют негативную динамику развития.

Наиболее пристальное внимание следует уделить нормативной базе, обеспечивающей информационную безопасность федерального органам государственной власти и государственным органам власти. Значимость проблемы обеспечения информационной безопасностью органов власти также обусловлена необходимостью уполномоченных предприятий в принятии эффективных управленческих решений. В дополнение, обеспечение

информационной безопасности органов власти напрямую связано с технологической безопасностью государства, а также особенную роль играют информационные ресурсы, которыми располагают представители органов власти и, которые могут представлять большой интерес для злоумышленников в целях доступа, сбора и искажения. В связи с этим, органами государственной власти уделяется особое внимание к вопросам совершенствования правового обеспечения высокого уровня защищенности информационной безопасности Российской Федерации.

В первую очередь, стоит отметить, что все вышеупомянутые документы также входят в нормативно-правовую базу, обеспечивающую информационную безопасность органам власти. Помимо Конституции РФ, УК РФ, ГК РФ, КоАП и ряда Федеральных Законов РФ, существует определенный массив правовых норм, который регламентирует процесс работы каждого органа в частности. В перечень документов, регламентирующих деятельность по защите информации органов федеральной и государственной власти, также входит большая часть документов Президента РФ, которые определяют направления деятельности в сфере безопасности, а также Концепции национальной безопасности.

Рассмотрим более подробно нормативно–правовую основу обеспечения информационной безопасности на примере Федеральной налоговой службы, поскольку именно этот федеральный орган власти хранит одно из наибольших информационных массивов, в том числе огромное количество персональных данных. В перечень проанализированных документов, обеспечивающих реализацию информационной безопасности в данном случае следует добавить:

- Налоговой Кодекс Российской Федерации;
- Федеральный Закон № 149 «Об информации, информационных технологиях и защите информации»;
- Федеральный Закон № 152 «О персональных данных»;
- Федеральный Закон № 2446-1 «О безопасности»;
- Федеральный Закон № 5485-1 «О государственной тайне»;

- «Положение о Федеральной налоговой службе»;
- Концепция информационной безопасности Федеральной налоговой службы;
- Специальные требования и рекомендации по защите информации, составляющей государственную тайну, от утечки по техническим каналам;
- Нормативно-методический документ «Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)».

Рассмотренный список документов является основным и не полным списком нормативно-правовых актов, которые регламентируют деятельность сотрудников Федеральной налоговой службы в области информационной безопасности.

Следует отметить, что такой обширный объем документов может являться причиной значительного усложнения идентификации границ полномочий и нарушений деятельности любого органа власти.

Таким образом, анализ существующей нормативно–правовой основы обеспечения информационной безопасности показал, что отечественная правовая система в области защищенности информации имеет большое количество изъянов. Количество уголовных преступлений и административных правонарушений, касающихся информационной безопасности личного, общественного и государственного характера с каждым годом увеличивается. Для достижения большей эффективности защиты конституционных прав от неправомерных действий необходимо регулярное, а главное своевременное усовершенствование нормативно-правовой системы.

Анализируя документы, которые регулируют правоотношения в сфере информационной безопасности Российской Федерации, можно отметить, что, как сильной, так и слабой стороной осуществления закона является большой массив юридической документации, отвечающий за нормы соблюдения установленных законов.

В дополнение, следует отметить недостаточную регулярность

модернизации существующих нормативно-правовых актов, что также оказывает негативное воздействие на реализацию конституционных прав человека, общества и государства, касающихся информационной защищенности.

2.2 Методы выявления актуальных угроз информационной безопасности на предприятии

Концепция управления информационной безопасностью определяет систему положений в проблематике регулирования и координации управления информационной безопасностью в Федеральной налоговой службе, а также при взаимодействии налоговых органов с Федеральными органами государственной власти и в процессе оказания услуг.

Процесс управления информационной безопасности в ФНС РФ регламентируется множеством нормативно-правовых документов, представляющих сложную иерархическую систему организационно-распорядительных документов.

Концепция системы управления информационной безопасностью определяет пути достижения необходимого уровня управления информационной безопасностью в процессе деятельности ФНС России.

Целью выявления угроз информационной безопасности является определение возможности нарушения основных свойств информации в процессе работы. Процесс выявления и определения угроз информационной безопасности должен нести регулярный и систематический характер, и должен осуществляться не только на этапе создания системы информационной безопасности, но и на этапе эксплуатации. Необходимо наладить процесс своевременного выявления и нейтрализации угроз информационной безопасности, который мог бы предотвратить возможный ущерб.

Экспертный метод

Оценка возможных угроз безопасности проводится путем формирования экспертной группы, которая проводит анализ уязвимостей. Благодаря качественному формированию экспертной группы можно снизить

уровень субъективности при оценке угроз. Состав экспертной группы формируется в соответствии с поставленными вопросами в области информационной безопасности и не может быть меньше количества трех человек. Также этот метод характерен низкими материальными затратами, поскольку задействованные эксперты являются сотрудниками службы [14].

Несмотря на достоинства данного метода, к этому методу можно отнести также ряд существенных недостатков. В первую очередь, это человеческий фактор, который подразумевает определенный уровень субъективности, что может привести к завышению или занижению экспертами прогнозов и предположений в процессе определения угроз информационной безопасности. Стоит отметить, что состав экспертной группы не могут составлять сотрудники, находящиеся на прямом подчинении, поскольку это может увеличить вероятность зависимой оценки. Также, эксперты не должны иметь личный, коммерческий или другой интерес в принятии решения, что также является сложной задачей для определения. Пример таблицы результатов экспертной оценки представлен на таблице 1.

Таблица 1 – Таблица результатов экспертной оценки

Эксперты	Значение оцениваемого параметра (этап №1)	Значение оцениваемого параметра (этап №2)
Эксперт 1		
Эксперт 2		
Эксперт n		
Итоговое значение		

Систематический метод

Систематический метод выявления угроз информационной безопасности предполагает непрерывный процесс, направленный на выявление и определение угроз, последующую идентификацию источника угрозы и оценку возможного ущерба в случае реализации угрозы. На регулярной основе проводится обзор и переоценка угроз информационной безопасности.

Обеспечение автоматизированного мониторинга может осуществляться как руководством налоговых органов, так и специализированным отделом по информационной безопасности. Мониторинг и контроль действий персонала также относится к систематическому методу выявление угроз. Попытка несанкционированного доступа сотрудника того или иного уровня к конфиденциальной информации будет зафиксирована в системе Федерального информационного ресурса, после чего последует процесс идентификации данного нарушения [15].

В процессе эксплуатации информационной системы соответствующий сотрудник имеет возможность менять ее базовую конфигурацию таким образом, чтобы обеспечить изменение приоритетов значимости обрабатываемой информации в соответствии с появлением новых угроз или новых требований на законодательном уровне. Необходимость переоценки угроз информационной безопасности также появляется в случаях изменения состава основных компонентов информационной системы, которые могли спровоцировать появление новых уязвимостей, новые сведения о возможных нарушителей и выявление уязвимостей.

Метод идентификации возможных источников угроз

Процесс определения угроз информационной безопасности предполагает систематическую идентификацию источников угроз, оценка возможности и, исходя из этого, выявление актуальных угроз информационной безопасности. Для осуществления идентификации угроз информационной безопасности в информационной системе ФНС необходимо выявить следующие критерии:

– вид и потенциал нарушителей, которые могут осуществить угрозу информационной безопасности;

– способы реализации угроз;

– уязвимости, которыми можно воспользоваться в целях нарушения, в том числе программные закладки;

– объекты воздействия, на которые направлена угроза.

– последствия реализации угроз информационной безопасности.

Метод оценки вероятности реализации угроз

В информационной системе ФНС с соответствующими функциональными характеристиками существует возможность оценки степени вероятности реализации анализируемой угрозы информационной безопасности нарушителем с соразмерным потенциалом и оценкой причиняемого ущерба. Высокий уровень актуальности исследуемой угрозы говорит о степени необходимости ее устранения.

Правовые методы

Правовые методы, как правило, направлены на устранение угроз антропогенного характера. В случае нарушения интересов предприятия правовые методы позволяют реализовать механизмы применения определенных санкций в отношение нарушителя. К основным правовым методам относятся [15]:

- установление порядка защиты и использования информации;
- определение области права обладания информацией;
- сохранение конфиденциальной информации;
- введение мер воздействия за противоправные действия в области использования информационных ресурсов;
- установление права судебной защиты интересов собственника.

Правовые методы противодействия угрозам информационной безопасности реализуются в ходе модернизации нормативно–правовой базы и обеспечивают информационную безопасность, а также способствуют формированию структуры управления.

Экономические методы

Экономические методы направлены на упразднение источников угроз антропогенного характера, а также на введение в действие механизмов устранения негативных последствий реализации угроз. К экономическим методам можно отнести:

- страхование средств обработки информации;
- страхование информационных рисков;

– введение системы надбавок и коэффициентов;

– введение механизма компенсации ущерба.

Таким образом, рассмотрены основные методы выявления угроз на предприятии. Помимо методов, необходимо проанализировать инструменты реализации выявления угроз информационной безопасности. Федеральная налоговая служба в процессе работы использует программный продукт Kaspersky Security, обеспечивающий безопасность основных свойств информации и осуществляющий выявление и устранение вредоносных программ.

Kaspersky Security является одним из самых современных антивирусных программ, обеспечивающий базовую защиту автоматизированного рабочего места. Для дальнейшей разработки комплексной методики необходимо рассмотреть достоинства и недостатки эксплуатации действующего программного продукта. К достоинствам использования Kaspersky Security в системе информационной безопасности ФНС можно отнести следующие положения:

– высокая скорость работы;

– высокая скорость проверки репутации программ и файлов автоматизированного рабочего места;

– задействование процесса мониторинга ссылок перед переходом на сайт;

– высокий уровень защиты автоматизированного рабочего места от вредоносных программ;

– блокировка нежелательного контента анти–баннером.

К минусам действующего программного продукта в системе информационной безопасности ФНС можно отнести:

– высокая стоимость программы, которая увеличивается с учетом большого количества территориальных подразделений ФНС;

– большой объем оперативной памяти занимаемой программы, что снижает производительность компьютера;

– полная проверка ПК подразумевает отключение всех действующих программ для уменьшения нагрузки, что является неприемлемой процедурой в определённых процессах работы.

Таким образом, проанализированные методы выявления угроз информационной безопасности являются актуальными и основными в процессе обеспечения информационной безопасности ФНС России. Данные методы имеют ряд достоинств и недостатков, и нуждаются в дальнейшем усовершенствовании для более эффективного обеспечения информационной безопасности предприятия.

2.3 Сравнительный анализ существующего программного обеспечения решающего поставленную задачу

В данном пункте рассматриваются методы и инструментальные средства для проведения автоматизированного аудита информационных активов предприятия, а также информационной безопасности в целом.

Представленные ниже программные продукты обеспечивают решение основных задач процесса проведения автоматизированного аудита и контроля информационных активов предприятия:

а). Dozor File Crawler – предназначен для оперативного мониторинга файловых ресурсов в локальной сети предприятия с возможностью активного противодействия нарушениям в области обеспечения информационной безопасности на предприятии. Интерфейс Dozor File Crawler представлен на рисунке 5.

Особенности Dozor File Crawler:

− сканирование узлов локальной сети, файловых хранилищ, расположенных в локальной сети предприятия;

− активное противодействие нарушениям правил использования, хранения и обработки информации ограниченного доступа.

− всевозможная настройка задач сканирования;

– оповещение администратора информационной безопасности о результатах выполнения задачи, в том числе о действиях, произведенных с файлами.

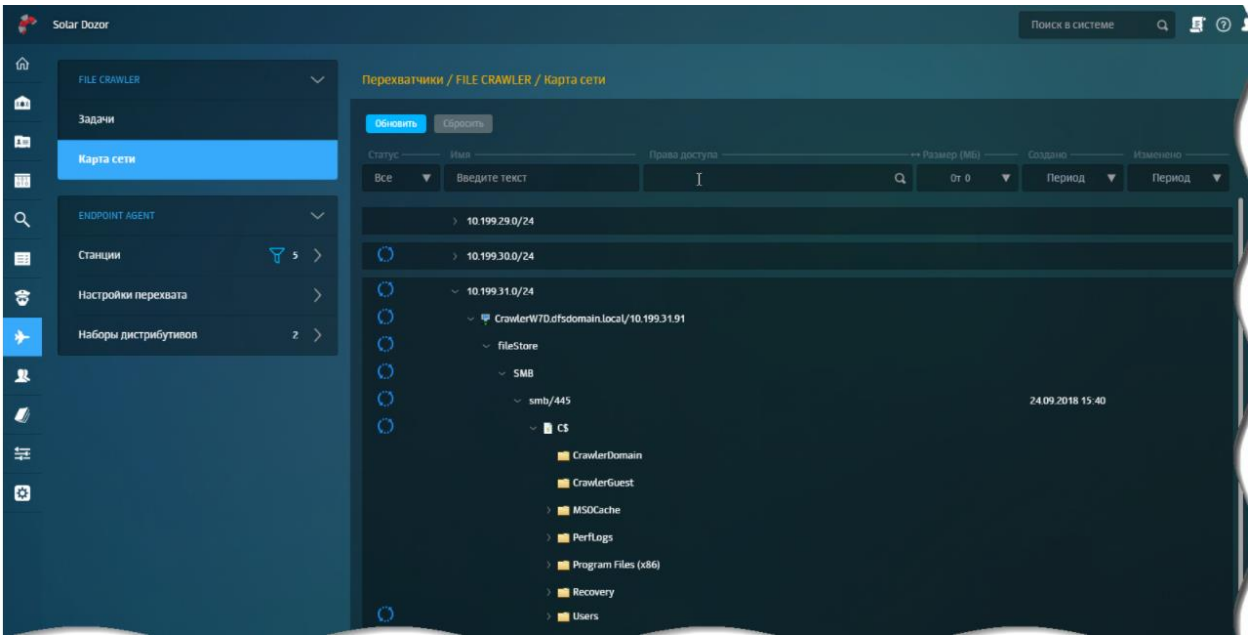

Рисунок 5 – Интерфейс Dozor File Crawler

б). Symantec DLP Network Discover – позволяет выявлять конфиденциальные данные, хранящиеся на локальных компьютерах пользователей информационной сети предприятия.

Особенности Symantec DLP Network Discover:

– возможность сканирования рабочих станций под управлением операционной системы Solaris, Windows, Linux, AIX;

– возможность проверки политик контроля доступа файлов.

Интерфейс Symantec DLP Network Discover подставлен на рисунке 6.

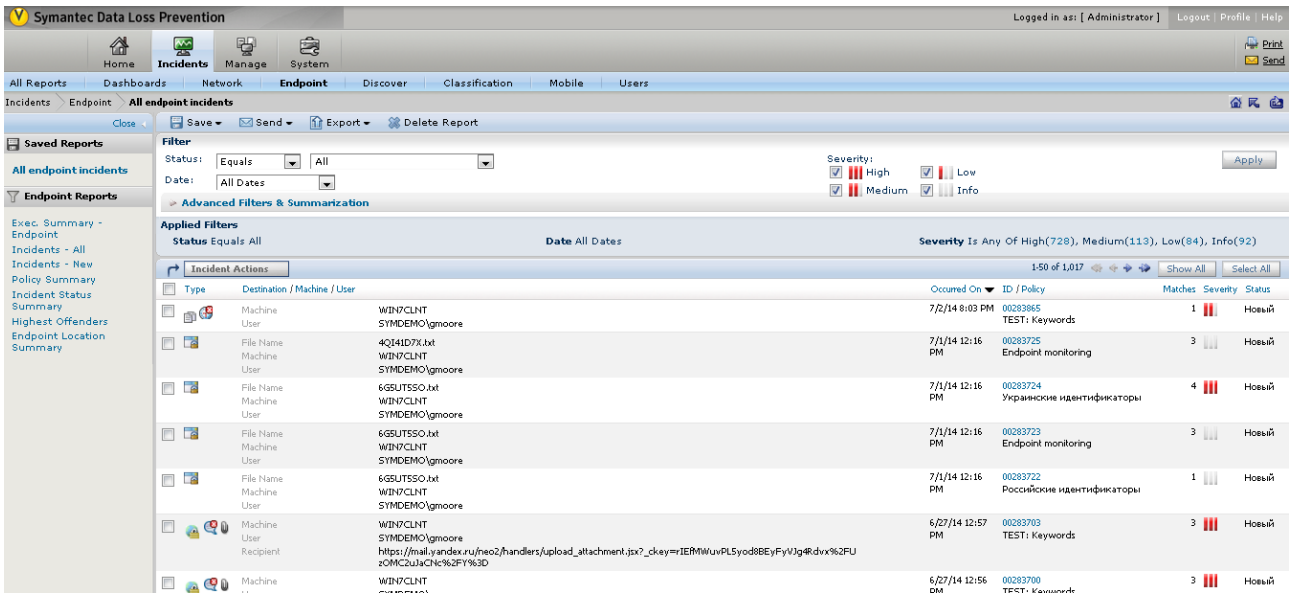

Рисунок 6 – Интерфейс Symantec DLP Network Discover

в). Zecurion Discovery – предоставляет возможность в режиме реального времени выявлять места хранения конфиденциальной информации в корпоративной сети с помощью специальных агентов. Система выполняет анализ данных со всех устройств, которые операционная система считает логическими дисками.

При этом в процессе работы определяется информация, которая должна защищаться в рамках политик безопасности организации. Интерфейс Zecurion Discovery представлен на рисунке 7.

Особенности Zecurion Zdiscovery:

– поддержка операционных систем Microsoft Windows 7/8/10; Server 2008 R2/2012/2012 R2/2016;

– выполнение различных действий с найденными файлами, например удаление или перемещение в специальные хранилища.

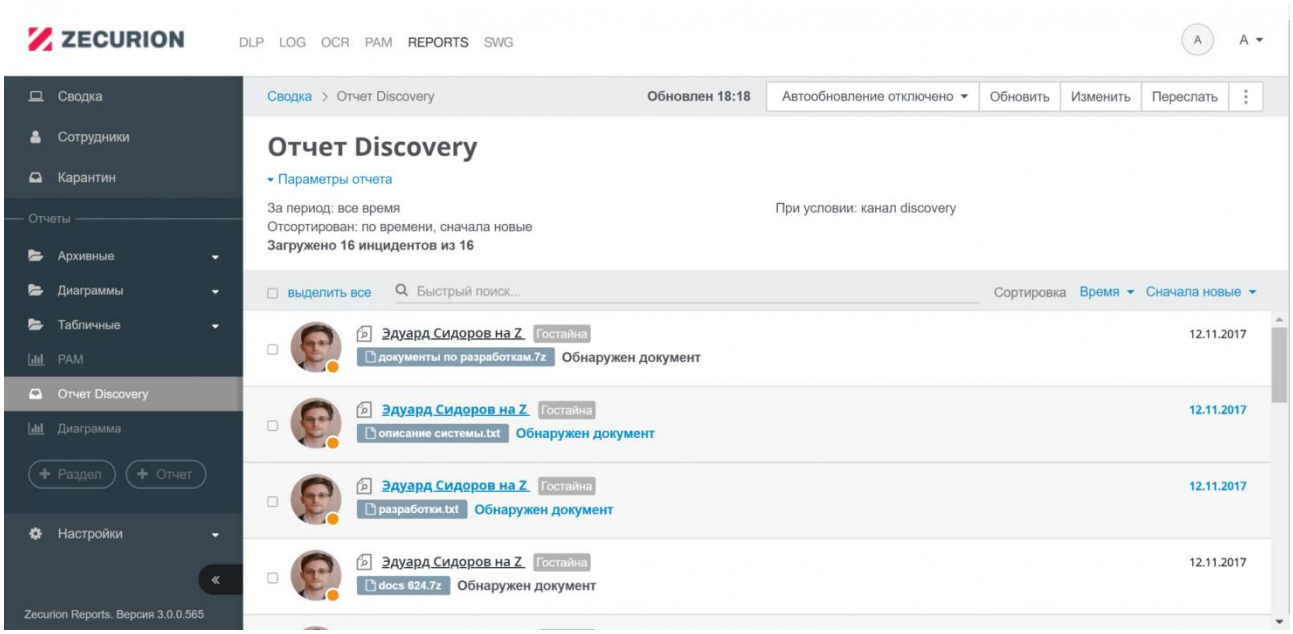

Рисунок 7 – Интерфейс Zecurion Zdiscovery

г). Гарда Предприятие – позволяет обнаружить файлы на компьютерах и серверах, размещенных в инфраструктуре организации. Управление поиском осуществляется с помощью специальных политик сканирования, в которых можно определить различные параметры и критерии поиска документов: поиск похожих документов, поиск по ключевым фразам и т. д. Интерфейс «Краулера» Гарда Предприятие представлен на рисунке 8.

Особенности «Краулера» Гарда Предприятие:

- осуществление поиска в автоматическом режиме;
- формирование инцидента при обнаружении подходящих документов и последующая отправка уведомления по электронной почте администратору безопасности;
- глубокая интеграция с возможностями операционной системы, что позволяет исключить нежелательную нагрузку на рабочие места сотрудников;
- возможности обработки и поиска данных по планировщику;
- минимальная нагрузка на контролируемые рабочие станции (учитывается текущая активность пользователя и периоды простоя).

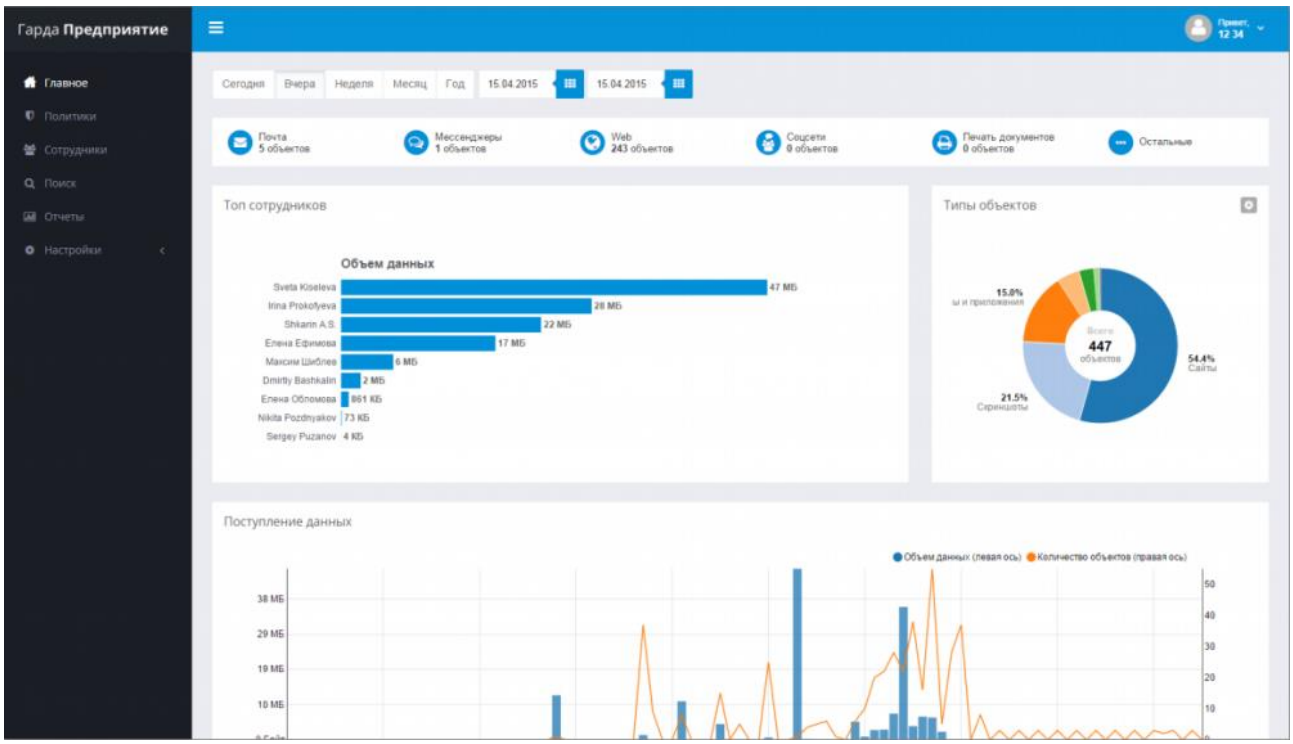

Рисунок 8 – Интерфейс «Краулера» Гарда Предприятие

С целью осуществления анализа основных возможностей программного обеспечения подготовлена сравнительная таблица 2.

Таблица 2 – Сравнительный анализ программных средств

Название программного средства	Осуществление поиска в автоматическом режиме	Возможность проверки политик контроля доступа и шифрования файлов	Portable – версия программы. (не требуется установка)	Гибкая настройка задач сканирования	Оповещение администратора информационной безопасности
Zecurion Zdiscovery	+	+	–	+	+
Dozor File Crawler	–	–	–	+	+
«Краулер» Гарда Предприятие	+	–	–	+	+
Symantec DLP Network Discover	+	–	+	–	–

Сравнительная таблица показывает основные характеристики исследуемых программных средств. Как видно из приведённой ниже таблицы,

каждое программное средство решает основные задачи процесса проведения автоматизированного аудита и контроля информационных активов предприятия, но ни одно программное средство не содержит необходимый набор функциональных требований, соответствующий специфике работы ФНС России.

Как альтернатива подобным средствам будет создано бесплатное программного обеспечение для автоматизированного аудита и контроля информационных активов предприятия, позволяющее проводить анализ информационных активов в соответствии со спецификой деятельности налоговых органов.

2.4 Обзор актуальных угроз информационной безопасности на предприятии

Массив информации, который обрабатывается в информационно телекоммуникационной системе ФНС России предоставляет потенциальную возможность для выявления угроз безопасности, которые в свою очередь, могут быть вызваны явлениями, процессами или действиями, провоцирующими причинение ущерба ФНС России.

Для объектов информатизации ФНС актуальными и основными источниками внешних антропогенных угроз безопасности информации являются:

– технические разведки иностранного происхождения, направленные на сведения, содержащие государственную тайну и на ключевую систему информационной инфраструктуры выше третьего уровня;

– злоумышленники, которые осуществляют преднамеренное воздействие деструктивного характера на информационные ресурсы;

– криминальные и террористические элементы;

– подрядчики, производящие монтажные и наладочные работы технического оборудования информационных систем ФНС;

– поставщики программно–технических средств и услуг. Основными источниками внутренних антропогенных угроз являются:

– сотрудники ФНС, действующие вне регламентированных полномочий, несущие преднамеренный характер угроз;

– сотрудники ФНС, действующие в рамках регламентированных полномочий, несущие непреднамеренный характер угроз.

Для объектов ФНС актуальными уязвимостями являются [16]:

– ошибки, совершенные в процессе проектирования объектов информатизации налоговых органов и телекоммуникационной инфраструктуры, включая физический износ оборудования, относительно небольшой промежуток времени наработки на отказ техники и программного обеспечения;

– недостаточная техническая укрепленность и недостаточный уровень организации системы охраны налоговых органов, включая нарушения эксплуатации технических средств, таких как: жизнеобеспечения и энергообеспечения;

– особенности сотрудников морального и физического плана, которые могут являться предпосылками к криминальному или террористическому воздействию;

– восприимчивость программного обеспечения к вирусам и вредоносным программам;

– возможность несанкционированной модификации программных вызовов, кода, использование среды программирования автоматизированной информационной системы;

– уязвимости системы защиты информации;

– несоответствующая настройка конфигурации программного обеспечения с регламентирующей правовой базой, включая средства защиты информации, неконтролируемость их изменений, не декларированные действия сотрудников при управлении программным оборудованием;

− неполная регламентация ответственности взаимодействия в договорах с подрядчиками;

− несоответствие деятельности и текущего состояния объекта защиты, отсутствие соответствующего контроля за исполнением сотрудниками ФНС России регламентов деятельности, включая установку стороннего программного обеспечения, нарушение регламента в процессе обмена информацией, уничтожения производственных отходов и носителей информации.

На основе рассмотренных источников и уязвимостей ФНС России в широком смысле можно сформировать более конкретизированный перечень угроз. Количество таких угроз для ФНС России составляет более 200 единиц, поэтому рассмотрим наиболее актуальные, применяя методику выявления угроз, описанную в предыдущем разделе, учитывая возможность и вероятность реализации, опасность, уровень исходной защищенности ИТ-инфраструктуры, обозначенный коэффициентом Y1. Степень исходной защищенности определяется с помощью семи технических и эксплуатационных показателей характеристик системы, для каждого из которых есть несколько вариантов значений. Из этих значений, в свою очередь, необходимо выбрать одно, которое больше остальных подходит для действующей информационной системы. Выбранному значению эквивалентен определенный уровень защищенности: низкий, средний или высокий. В таблице 3 представлены угрозы с наивысшим уровнем актуальности и высоким уровнем возможной реализации.

Таблица 3 – Перечень угроз с наивысшим уровнем возможной реализации

Наименование угрозы безопасности информации	**Опасность**	**Вероятность реализации**	**Y1**	**Возможность реализации**
Угроза обнаружения открытых портов и идентификации привязанных к нему сетевых служб	Средняя	Высокая	1	Очень высокая

Продолжение таблицы 3

Угроза маскирования действий вредоносного кода	Высокая	Средняя	0,75	Высокая
Угроза обнаружения хостов	Средняя	Высокая	1	Очень высокая
Угроза скрытного включения вычислительного устройства в состав бот–сети	Средняя	Средняя	0,75	Высокая
Угроза определения топологии вычислительной сети	Средняя	Высокая	1	Очень высокая
Угроза передачи данных по скрытым каналам	Средняя	Высокая	1	Очень высокая
Угроза перехвата исключения/сигнала из привилегированного блока функций	Высокая	Средняя	0,75	Высокая
Угроза несанкционированного использования системных и сетевых утилит	Высокая	Средняя	0,75	Высокая
Угроза повреждения системного реестра	Высокая	Высокая	1	Очень высокая
Угроза повышения привилегий	Высокая	Высокая	1	Очень высокая
Угроза подмены доверенного пользователя	Высокая	Высокая	1	Очень высокая
Угроза сканирования веб–сервисов	Средняя	Высокая	1	Очень высокая
Угроза удаления аутентификационной информации	Высокая	Высокая	1	Очень высокая
Угроза «спама» вебсервера	Средняя	Высокая	1	Очень высокая
Угроза использования уязвимых версий программного обеспечения	Высокая	Высокая	1	Очень высокая

Таким образом, проанализировав перечень угроз, был выявлен список наиболее вероятных и актуальных угроз для безопасности информации Федеральной налоговой службы. Можно сказать, что количество возможных угроз очень велико и разобщено, поэтому своевременный процесс выявления

возможных угроз представляется крайне затруднительным. Такой обширный спектр возможных угроз и усложненный процесс выявления может повлечь за собой существенный ущерб, в том числе экономический.

Методика определения уровня защищенности и актуальности той или иной угрозы также содержит определенные сложности. К одному показателю может подойти сразу несколько значений, а может не подойти ни одного, что также создает сложности в вычислениях. Актуальность угрозы также зависит от предпосылок, но неактуальные угрозы также должны быть включены в список угроз, но с нулевым значением вероятности, это предполагает произведение большого количества лишних расчетов для угроз, не имеющих никаких предпосылок [17].

Также вызывает сложности процесс определения показателя «опасность угрозы». Высокая, средняя и низкая опасность определяется в соотношении масштаба последствий, которые могут произойти при реализации той или иной угрозы. В соответствии с действующей методикой определить значимость или незначительность негативных последствий можно с помощью опроса экспертов. Анализ метода экспертной оценки, в свою очередь, показал большое количество недостатков использования данного метода. Данный метод отличается высоким уровнем субъективности оценки и наличием человеческого фактора, который может стать причиной определения степени опасности угрозы информационной безопасности, как низкой, с целью сокращения списка актуальных угроз.

Действующая методика привязана к субъектам персональных данных и к самим персональным данным, что приводит к значительным сложностям в процессе разработки моделей угроз для информационных систем без персональных данных.

3 ПРОЕКТИРОВАНИЕ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

3.1 Постановка целей и задач разработки программного обеспечения

При реализации функций программного обеспечения для автоматизированного аудита и контроля информационных активов предприятия, отвечающее за выполнение этих функций, должно обеспечивать:

- осуществление поиска критической информации в автоматическом режиме;
- возможность проверки политик контроля доступа и шифрования файлов;
- использование portable – версии программы (не требующей установки);
- гибкую настройку задач сканирования;
- оповещение администратора информационной безопасности;
- определение любых изменений (удаление, изменение или добавление новых правил) ключевых элементов в конфигурации политик устройств в локальной сети;
- создание отчетов (в виде журналов) по выявленным инцидентам информационной безопасности;
- выдачу оповещений по параметрам работы, если полученные значения отличаются от установленных эталонных значений.

3.2 Выбор модели жизненного цикла программного обеспечения

Понятие жизненного цикла проекта подразумевает под собой определенную последовательность этапов по реализации той или иной идеи касательно производственного или управленческого процесса. Важность данного понятия обуславливается тем, что оно фиксирует продолжительность проекта, четко обозначая сроки его выполнения; позволяет детализировать процесс реализации замысла, разбивая его на конкретные фазы; дает возможность четко определить количество задействованного персонала, а также необходимые ресурсы; облегчает процедуру контроля. Жизненный цикл

проекта – это совокупность фаз, через которые реализуется первоначальный замысел. Такое разделение важно не только с теоретической, но также и с практической точки зрения, ведь оно дает возможность лучше контролировать процесс производства программного продукта.

Наибольшее распространение получили модели жизненного цикла разработки программного продукта представленные в таблице 4.

Таблица 4 – Краткие характеристики каждой из перечисленных моделей

Название	Характеристики
Каскадная модель	Прямолинейная и простая в использовании. Необходим постоянный жесткий контроль за ходом работы. Разрабатываемое программное обеспечение не доступно для изменений
V–образная модель	Простая в использовании. Особое значение придается тестированию и сравнению результатов фаз тестирования и проектирования
Модель прототипирования	Создается «быстрая» частичная реализация системы до составления окончательных требований. Обеспечивается обратная связь между пользователями и разработчиками в процессе выполнения проекта. Используемые требования не полные
Модель быстрой разработки приложений	Проектные группы небольшие и составлены из высококвалифицированных специалистов. Уменьшенное время цикла разработки (до 3 месяцев) и улучшенная производительность. Повторное использование кода и автоматизация процесса разработки
Многопроходная модель	Быстро создается работающая система. Уменьшается возможность внесения изменений в процессе разработки. Невозможен переход от текущей реализации к новой версии в течение построения текущей частичной реализации
Спиральная модель	Охватывает каскадную модель. Расчленяет фазы на меньшие части. Позволяет гибко выполнять проектирование. Анализирует риски и управляет ими.

Каскадная модель – модель процесса разработки программного обеспечения, жизненный цикл которой выглядит как поток, последовательно проходящий фазы анализа требований, проектирования. реализации, тестирования, интеграции и поддержки. В каскадной модели все шаги должны быть завершены до начала разработки. Одним из основных предварительных условий каскадной модели является получение одобрения на каждом этапе, прежде чем команда сможет перейти к следующему. Этот подход может быть

эффективным в снижении рисков в жизненном цикле разработки программного обеспечения.

Каскадная модель занимает значимое место совершенно в различных сферах деятельности, таких как строительство, военная промышленность. Отличительным свойством каскадной модели является формализация, что особенно ценно в работе с государственных структур и крупных компаний, для которых формализация и документация процессов является первоочередной целью, даже в ущерб срокам/стоимости/качеству продукта.

Выделяются шесть последовательных фаз (в некоторых источниках может быть пять) представленных на рисунке 8. Отличительной особенностью подхода является то, что переход к следующей фазе происходит только после завершения предыдущей, но возможны некоторые отклонения, например возврат к предыдущим фазам в случае возникновения проблем или обнаружения недостатков.

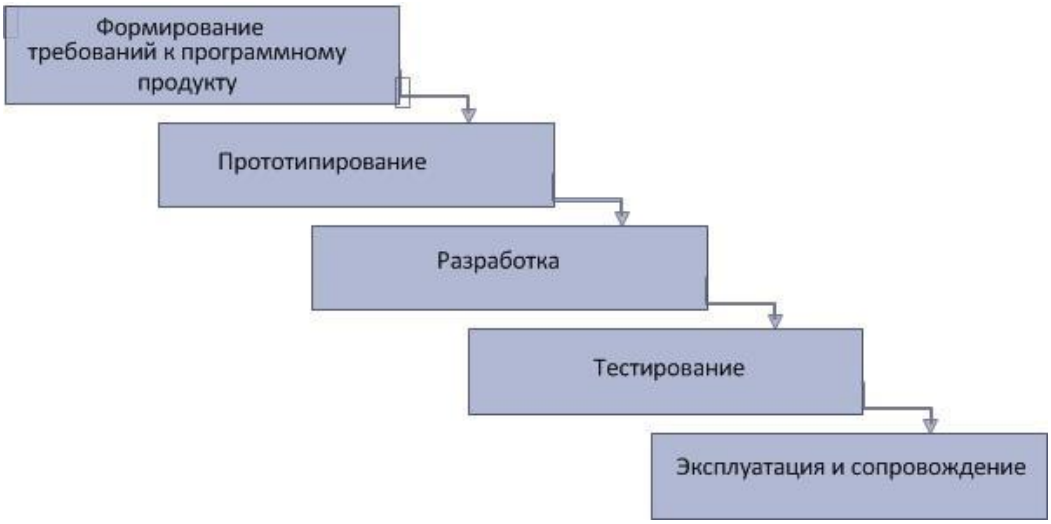

Рисунок 8 – Каскадная модель

Спиральная модель является универсальной моделью жизненного цикла разработки программного обеспечения. Подобно итерационной модели, она подчеркивает значение меньших циклов в рамках больших циклов. Спиральная модель тесно объединяет все ключевые этапы процесса разработки. Эта модель жизненного цикла разработки программного обеспечения исключает сложности

любого традиционного жизненного цикла разработки программного обеспечения. Жизненный цикл – на каждом витке спирали выполняется создание очередной версии продукта, уточняются требования проекта, определяется его качество и планируются работы следующего витка. Особое внимание уделяется начальным этапам разработки – анализу и проектированию, где реализуемость тех или иных технических решений проверяется и обосновывается посредством создания прототипов.

V-образная модель имеет более приближенный к современным методам алгоритм, однако все еще имеет ряд недостатков. Является одной из основных практик экстремального программирования. V-образная модель похожа на каскадную модель и может рассматриваться как его продолжение. Поэтому методологической основой V-образной модели является гарантия выполнения задач на одном этапе перед переходом к следующему. Эта модель также делит процесс разработки на различные задачи. Еще одной особенностью V-образной модели является постоянное тестирование, что выделяет ее среди некоторых других моделей жизненного цикла разработки.

Представленную на рисунке 9 модель, целесообразно использовать при разработке программных продуктов, главным требованием для которых является высокая надежность.

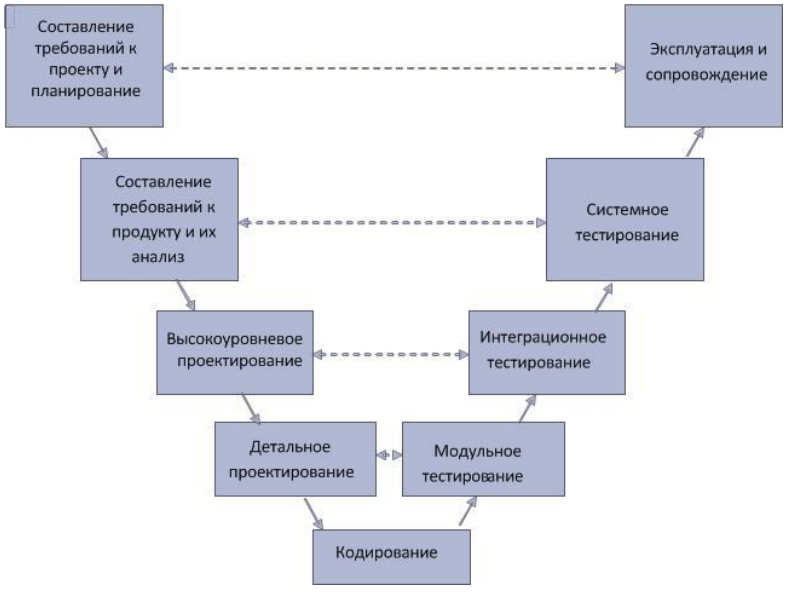

Рисунок 9 – V–образная модель

Модель прототипирования включает в себя несколько прототипов. Как правило, под прототипом понимается действующий программный модуль, обеспечивающий выполнение заранее определённых функции и реализацию внешних интерфейсов разрабатываемого программного обеспечения.

Использование модели прототипирования позволяет уже на этапе разработки требований создавать работающие программные модули, реализующие отдельные функции. Потенциальные пользователи работают с этим прототипом, определяя его преимущества и недостатки, о результатах сообщают разработчикам программного обеспечения. Таким образом, определяется взаимодействие между пользователями и разработчиками, которое используется для изменения или корректировки спецификации требований к программному обеспечению. В результате такой работы реализуемый проект будет отражать реальные потребности пользователей [20].

Схема жизненного цикла модели прототипирования представлена на рисунке 10.

Рисунок 10 – Модель прототипирования

Итерационная модель имеет много циклов разработки программного обеспечения, которые сегментированы на более мелкие циклы. Кроме того, эта модель обеспечивает надежный старт для программного продукта с помощью опробования. Среди конкретных примеров моделей жизненного цикла

разработки программного обеспечения здесь рациональный унифицированный процесс позволяет избежать ограничений некоторых других моделей жизненного цикла разработки программного обеспечения. Поскольку метод разработки динамических систем, используемый в этой модели, делит цикл на несколько более мелких, что позволяет осуществлять микроменеджмент, итеративная модель – это один из самых надежных подходов к процессу разработки.

Выбор модели жизненного цикла разработки можно осуществлять исходя из результатов анализа следующих характеристик:

- количество разработчиков принимаемых участие в реализации проекта;
- полнота и сложность реализации требований предъявляемых к разрабатываемому программному обеспечению;
- вероятных рисков и типа проекта.

Процедуру выборы модели жизненного цикла необходимо осуществляться на основе рассмотрения не отдельных критериев, а их комплекса. При этом существенную роль будут играть особенности реальной ситуации. Для наглядного представления составлена сводная таблица 5, которая включает в себя преимущества и недостатки всех перечисленных моделей жизненного цикла.

Таблица 5 – Преимущества и недостатки моделей жизненного цикла

Модель	Преимущества	Недостатки
Каскадная	- на каждом этапе формируется законченный набор проектной документации, отвечающий критериям полноты и согласованности; - на заключительных этапах жизненного цикла разрабатывается документация, охватывающая все предусмотренные стандартами виды обеспечения ИС – организационное, методическое, информационное, программное, аппаратное; - выполняемые в логической последовательности этапы работ позволяют планировать сроки завершения и оценивать затраты.	- существенная задержка в получении результатов; - ошибки и недоработки на любом из этапов выявляются, как правило, на последующих этапах работ, что приводит к необходимости возврата на предыдущие стадии; - сложность распараллеливания работ по проекту; - чрезмерная информационная насыщенность каждого из этапов; - сложность управления проектом; - высокий уровень риска и ненадежность инвестиций.

Продолжение таблицы 5

Спиральная	- наличие действий по анализу рисков, что обеспечивает их сокращение и заблаговременное определение непреодолимых рисков; обеспечение разбиения большого потенциального объема работ по выполнению проекта на небольшие части; - первоочередность реализации решающих функций с высокой степенью риска, что позволяет при необходимости остановить работы над проектом на ранних циклах модели и уменьшить расходы; - возможность гибкого проектирования, основанная на преимуществах каскадной модели при одновременном разрешении итераций; - реализация связи с пользователем с высокой частотой и на ранних этапах модели, что обеспечивает создание нужного продукта высокого качества; приводит к их общему сокращению.	- высокая стоимость модели за счет стоимости и дополнительных временных затрат на планирование, определение целей, выполнение анализа рисков и прототипирование при прохождении каждого цикла спирали; - неоправданно высокая стоимость модели для проектов, имеющих низкую степень риска или небольшие размеры; усложненность структуры модели, что приводит к сложности ее использования разработчиками, менеджерами и заказчиками; - необходимость в высокопрофессиональных знаниях для оценки рисков; - возможность отдаления окончания работы над проектом в связи с желанием заказчика улучшать каждую созданную версию;
V-образная	- планирование на ранних стадиях разработки системы ее тестирования; - обеспечение аттестации и верификации всех промежуточных результатов разработки; - упрощение (по сравнению с каскадной моделью) отслеживания хода процесса разработки, возможность более реального использования графика проекта; - простота в использовании.	- сложность поддержки параллельных событий; - непредусмотренность итераций между фазами; - невозможность внесения динамических изменений в требования на разных этапах жизненного цикла; - поздние сроки тестирования требований в жизненном цикле, что оказывает существенное влияние на график выполнения проекта при необходимости выполнить их изменения.
Итерационная	- снижение воздействия серьёзных рисков на ранних стадиях проекта, что ведет к минимизации затрат на их устранение; - организация эффективной обратной связи проектной команды с потребителем и создание продукта, реально отвечающего его потребностям; - акцент усилий на наиболее важные и критичные направления проекта.	- целостное понимание возможностей и ограничений проекта очень долгое время отсутствует; - при итерациях приходится отбрасывать часть сделанной ранее работы.

В результате рассмотрения всех видов моделей жизненного цикла и анализа преимуществ и недостатков, принято решение, использовать

каскадную модель в связи с реализаций логической последовательности этапов разработки программного обеспечения, позволяющей планировать работы и регулировать сроки завершения разработки программного обеспечения.

3.3 Обоснование выбора языка программирования

В рамках реализации проектируемого программного обеспечения выявлены следующие требования к среде разработки:

- поддержка объектно-ориентированного программирования;
- возможность построения графического интерфейса;
- возможность создания исполняемого файла, не привязанного к среде разработки.

В настоящее время существует множество графических сред разработки имеющих различный интерфейс и методы программирования на различных языках. Наиболее популярными средствами разработки выступают:

- Microsoft Visual C++;
- Borland Delphi;
- Borland C++ Builder.

Это языки высокого уровня, поддерживающие объектно-ориентированное программирование.

Во всем мире объектно-ориентированное программирование находит место в различных областях, таких как управление банковскими операциями и переводами, управление жилищно-коммунальным хозяйством. Реализация моего программного обеспечения будет осуществляться с помощью Borland C++ Builder.

Система объектно-ориентированного программирования Borland C++ Builder, предназначена для операционных систем Windows. Интегрированная среда C++ Builder обеспечивает скорость визуальной разработки, продуктивность повторно используемых компонентов в сочетании с мощью языковых средств C++, усовершенствованными инструментами и разномасштабными средствами доступа к базам данных.

Профессиональные средства языка C++ интегрированы в визуальную среду разработки. C++Builder предоставляет быстродействующий компилятор с языка Borland C++, эффективный инкрементальный загрузчик и гибкие средства отладки как на уровне исходных инструкций, так и на уровне ассемблерных команд – в расчете удовлетворить высокие требования программистов–профессионалов.

C++ Builder может быть использован везде, где требуется дополнить существующие приложения расширенным стандартом языка C++, повысить быстродействие и придать пользовательскому интерфейсу качества профессионального уровня.

Профессиональные средства языка C++ интегрированы в визуальную среду разработки. C++Builder предоставляет быстродействующий компилятор с языка Borland C++, эффективный инкрементальный загрузчик и гибкие средства отладки как на уровне исходных инструкций, так и на уровне ассемблерных команд – в расчете удовлетворить высокие требования программистов-профессионалов.

3.4 Архитектурный проект программного обеспечения

3.4.1 Диаграмма вариантов использования

Визуальное моделирование в UML можно представить как некоторый процесс поуровневого спуска от наиболее обшей и абстрактной концептуальной модели исходной системы к логической, а затем и к физической модели соответствующей программной системы. Диаграмма вариантов использования является исходным концептуальным представлением или концептуальной моделью системы в процессе ее проектирования и разработки.

Диаграмма вариантов использования (сценариев поведения, прецедентов) является исходным концептуальным представлением системы в процессе ее проектирования и разработки.

Варианты использования используются для представления функций высокого уровня и того, как пользователь будет обращаться с

системой. Вариант использования представляет отдельную функциональность системы, компонента, пакета или класса. Он обозначен овальной формой с названием варианта использования, написанным внутри овальной формы.

Вариант использования (use-case) дает возможность понять, каким образом действуют участники процесса, и за счет этого определить их взаимодействие и влияние на процесс.

При работе с вариантами использования системы важно помнить:

- каждый прецедент относится как минимум к одному действующему лицу;
- каждый прецедент имеет инициатора;
- каждый прецедент приводит к соответствующему результату.

С программным обеспечением могут взаимодействовать несколько категорий пользователей, а именно:

а) Администратор информационной безопасности:

- осуществляет работу по разграничению прав доступа субъектов к информационным ресурсам;
- производит модерацию действий пользователей в информационной системе;
- формирует реестр разрешенных к использованию программных и аппаратных средств;
- присваивает и изменяет полномочия пользователей информационной системы в связи с кадровыми изменениями;
- анализирует подключенные аппаратные средства;
- анализирует содержимое системного журнала;
- производит аудит информационных активов;
- создаёт метки для проверки информационных активов;
- осуществляет работы по недопущению инцидентов информационной безопасности посредством проверки сводных отчетов, предоставляемых программным обеспечением.

б) Системный администратор:

– производит установку и первоначальную настройку программного обеспечения на автоматизированные рабочие места сотрудников;

– поддерживает бесперебойное функционирование программного обеспечения;

– обнаружение уязвимостей и мгновенное оповещение администратора информационной безопасности.

в) Пользователь информационных ресурсов:

– работа в информационной системе;

– просмотр предоставляемых прав;

– соблюдение политики безопасности;

– самоконтроль совершаемых действий в информационной системе.

Основной назначение диаграммы – описание функциональности и поведения, позволяющее конченому пользователю и разработчику обсуждать проектируемую или существующую систему.

Диаграмма вариантов использования представлена на рисунках 11 и 12.

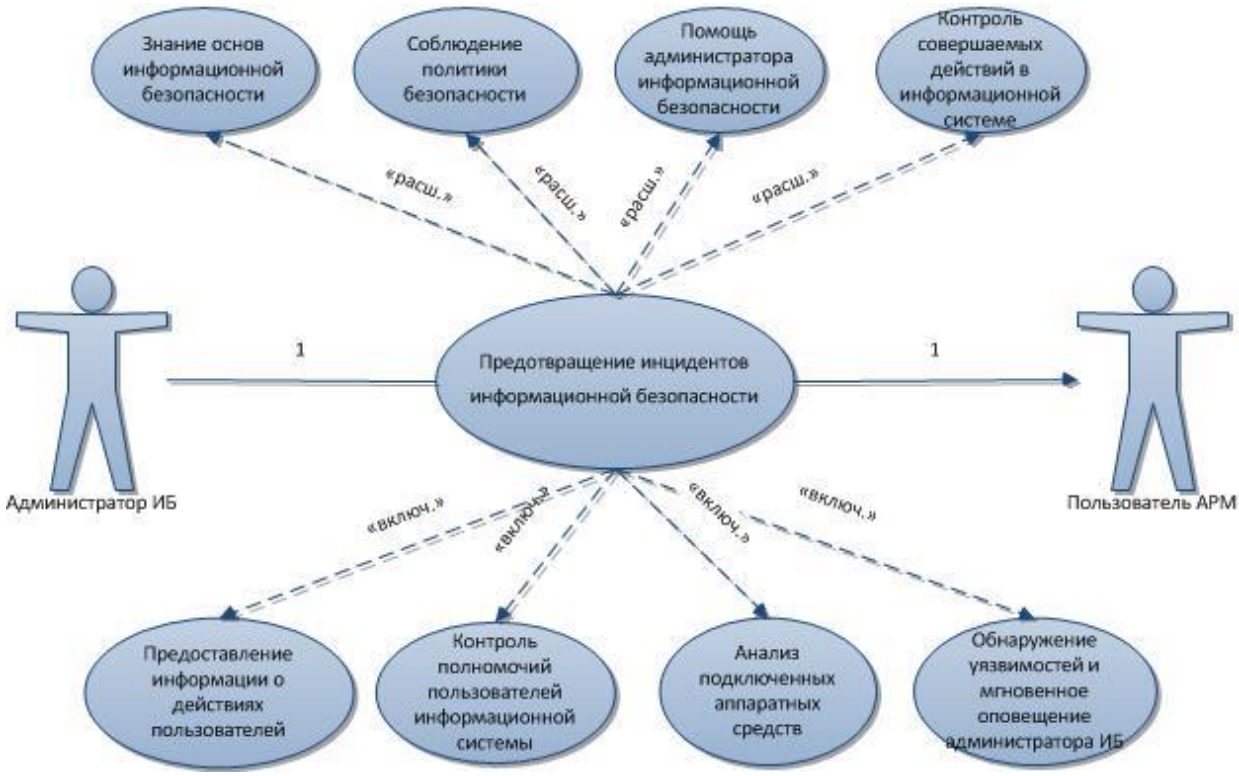

Рисунок 11 – Диаграмма вариантов использования

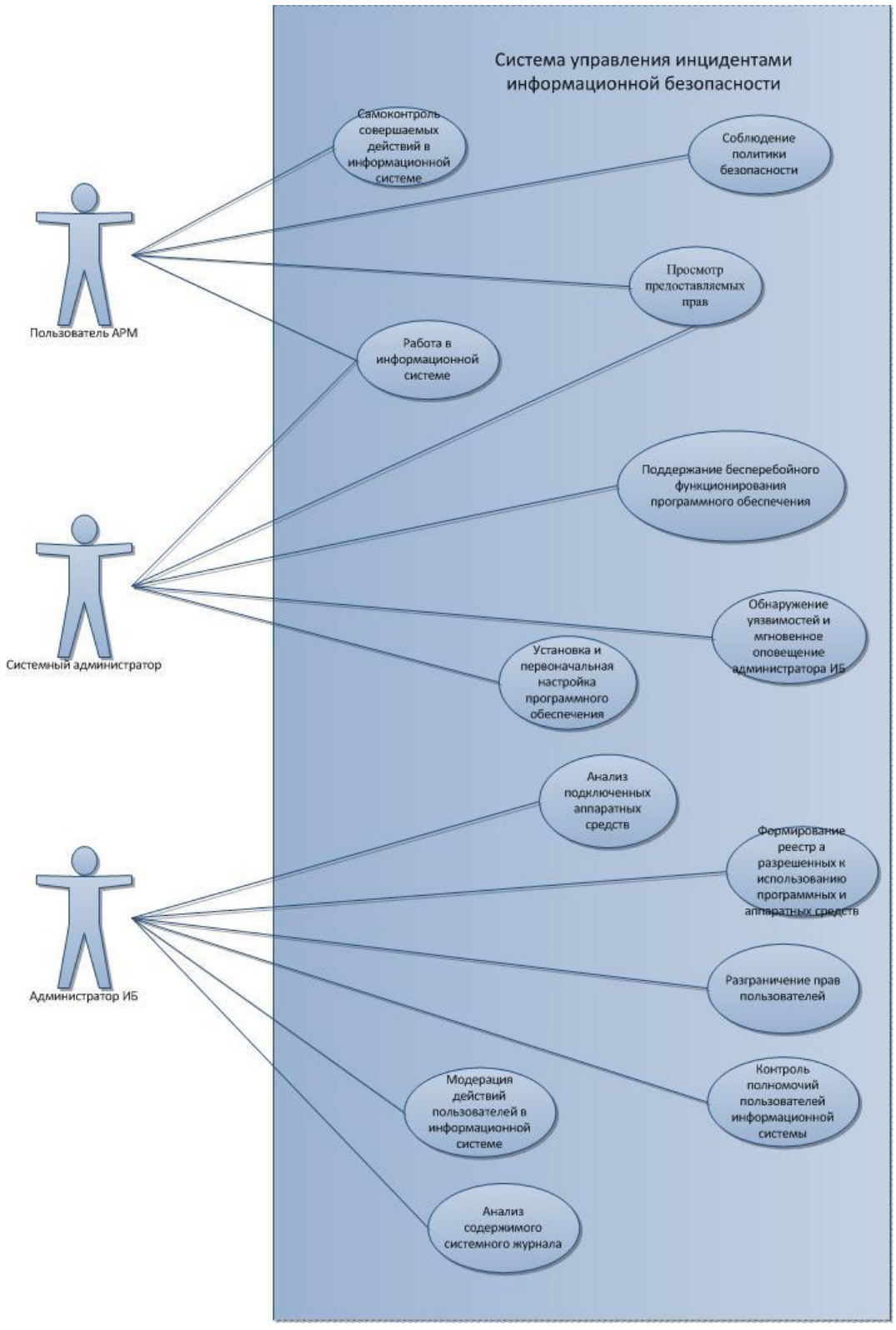

Рисунок 12 – Диаграмма вариантов использования

3.4.2 Диаграмма последовательности

Диаграмма последовательности – (UML-диаграмма, на которой для некоторого набора объектов на единой временной оси показан жизненный цикл

объекта (создание-деятельность-уничтожение некой сущности) и взаимодействие актеров (действующих лиц) информационной системы в рамках прецедента.

Диаграмма последовательности наглядно отображает временной аспект взаимодействия. Она имеет два измерения. Одно измерение (слева направо) указывает на порядок вовлечения экземпляров сущностей во взаимодействие. Крайним слева на диаграмме отображается экземпляр действующего лица или объекта, который является инициаторов взаимодействия. Второе измерение (сверху вниз) указывает на порядок обмена сообщениями.

После запуска программного обеспечения администратору требуется произвести установку и первичную настройку программного обеспечения. После успешной установки, администратор может приступить к формированию реестра пользователей и работе по разграничению прав доступа. Далее необходимо составить план защиты информационных ресурсов и произвести установку требований политики информационной безопасности предприятия.

Диаграмма последовательности действий администратора представлена на рисунке 13.

Рисунок 13 – Диаграмма последовательности

После успешной настройки программного обеспечения работа администратору необходимо производить работы по:

– выявлению и устранению инцидентов безопасности, уязвимостей;

– своевременному внесению изменений в реестр прав доступа;

– анализу сводных отчетов.

Диаграмма последовательности программного обеспечения представлена на рисунке 14.

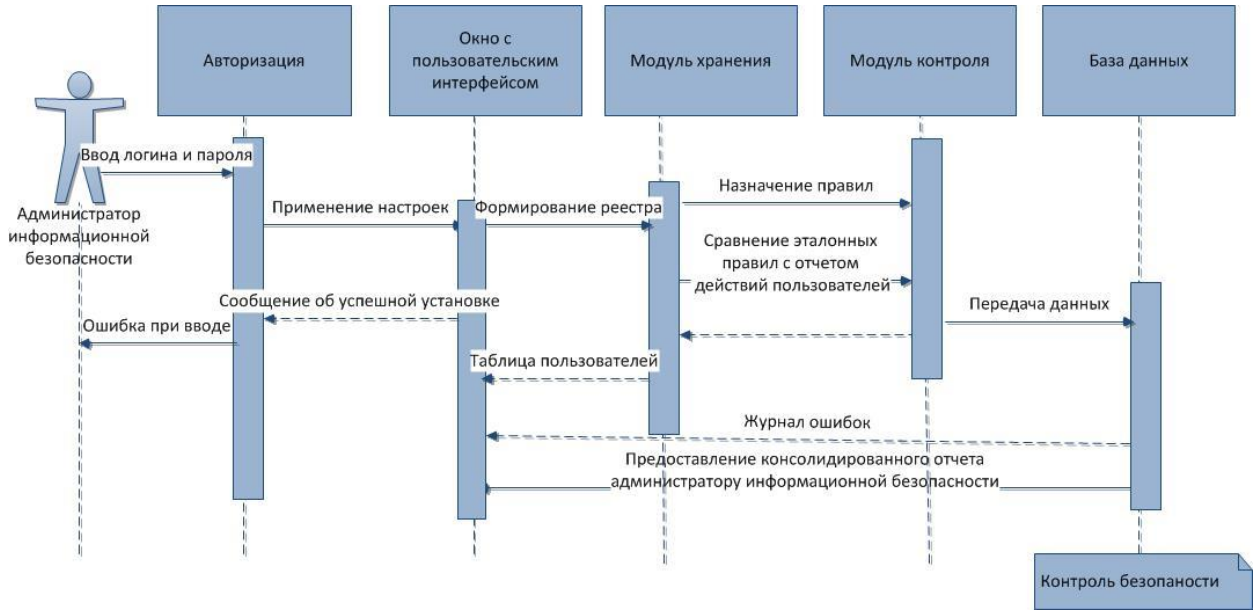

Рисунок 14 – Диаграмма последовательности

3.4.3 Диаграмма состояний

Диаграмма состояний используется для описания поведения сложных систем. Они определяют все возможные состояния, в которых может находится объект, а также процесс смены состояний объекта в результате некоторых событий.

При использовании диаграммы состояний важно следовать следующим правилам:

– диаграмма состояний должна создаваться только для объектов, обладающих реактивным поведением. Не следует делать диаграмму автоматов для всех классов или объектов, достаточно выбрать только основные классы или объекты, обладающие сложным поведением;

− диаграмма состояний должна быть сосредоточена на описании только одного аспекта поведения объекта. Следует создавать диаграмму автомата, моделирующую поведение только одного объекта. Если необходимо показать поведение нескольких, взаимосвязанных объектов, допустимо создавать для них диаграмму состояний в рамках определенного варианта использования (диаграмма состояний для варианта использования);

− на диаграмме состояний целесообразно использовать только те элементы, которые существенны для понимания описываемого аспекта.

Таким образом, на диаграмме состояний можно увидеть следующие аспекты:

− сообщения, побуждающие объект к действию;

− действия, которые вызываются сообщениями (методы) – зачастую это передача сообщения следующему объекты или возвращение определенных данных объекта;

− последовательность обмена сообщениями между объектами.

Разрабатываемое программное обеспечение может находиться в 4 состояниях:

– ожидание ввода данных;

– формирование реестра;

– сравнение получаемых данных с эталонными значениями (заданными администратором);

– анализ получаемой информации;

– формирование консолидированного отчёта;

– сохранение в БД.

Диаграмма состояний программного обеспечения и диаграмма состояний администратора информационной безопасности представлены на рисунке 15.

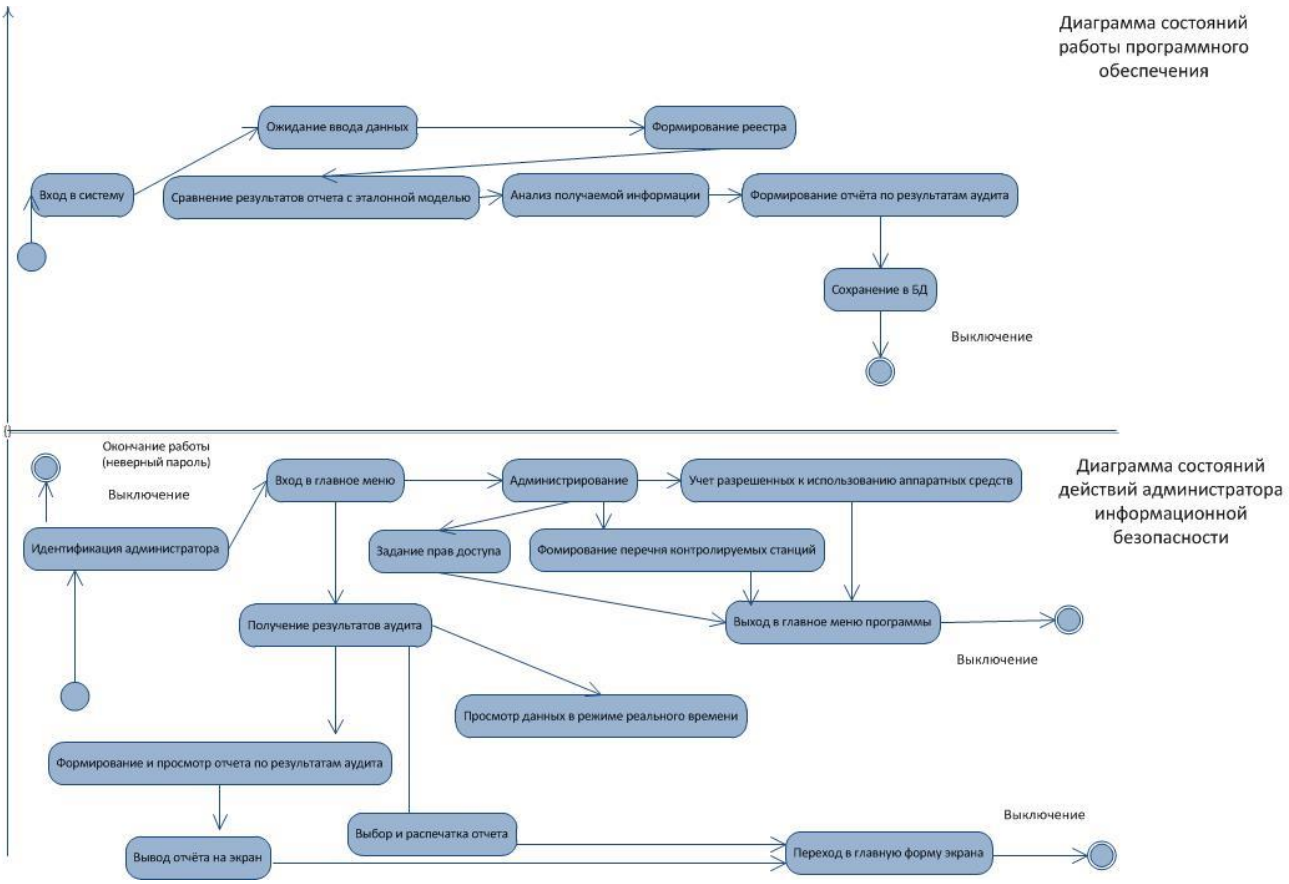

Рисунок 15 – Диаграмма состояний

На стадии ожидания ввода данных программа готова получать данные от администратора. После получения информации происходит переход к состоянию формирования реестра, в которым происходит сохранение данных о сотрудниках, прав доступа, списка аппаратных средств. После того, как все необходимы настройки выполнены, программа переходит к анализу действий пользователей в информационных системах и сопоставление этих действий с заданными значениями (эталонной моделью). После анализа программа готова предоставить администратору консолидированный отчет в разрезе времени, пользователей и действий, совершенных в информационных системах. После этого происходит сохранения отчета и данных.

3.4.4 Диаграмма активности

Диаграмма активности – UML-диаграмма, на которой показаны действия, состояния которых описаны на диаграмме состояний. Под деятельностью понимается спецификация исполняемого поведения в виде координированного

последовательного и параллельного выполнения подчинённых элементов – вложенных видов деятельности и отдельных действий action, соединённых между собой потоками, которые идут от выходов одного узла ко входам другого.

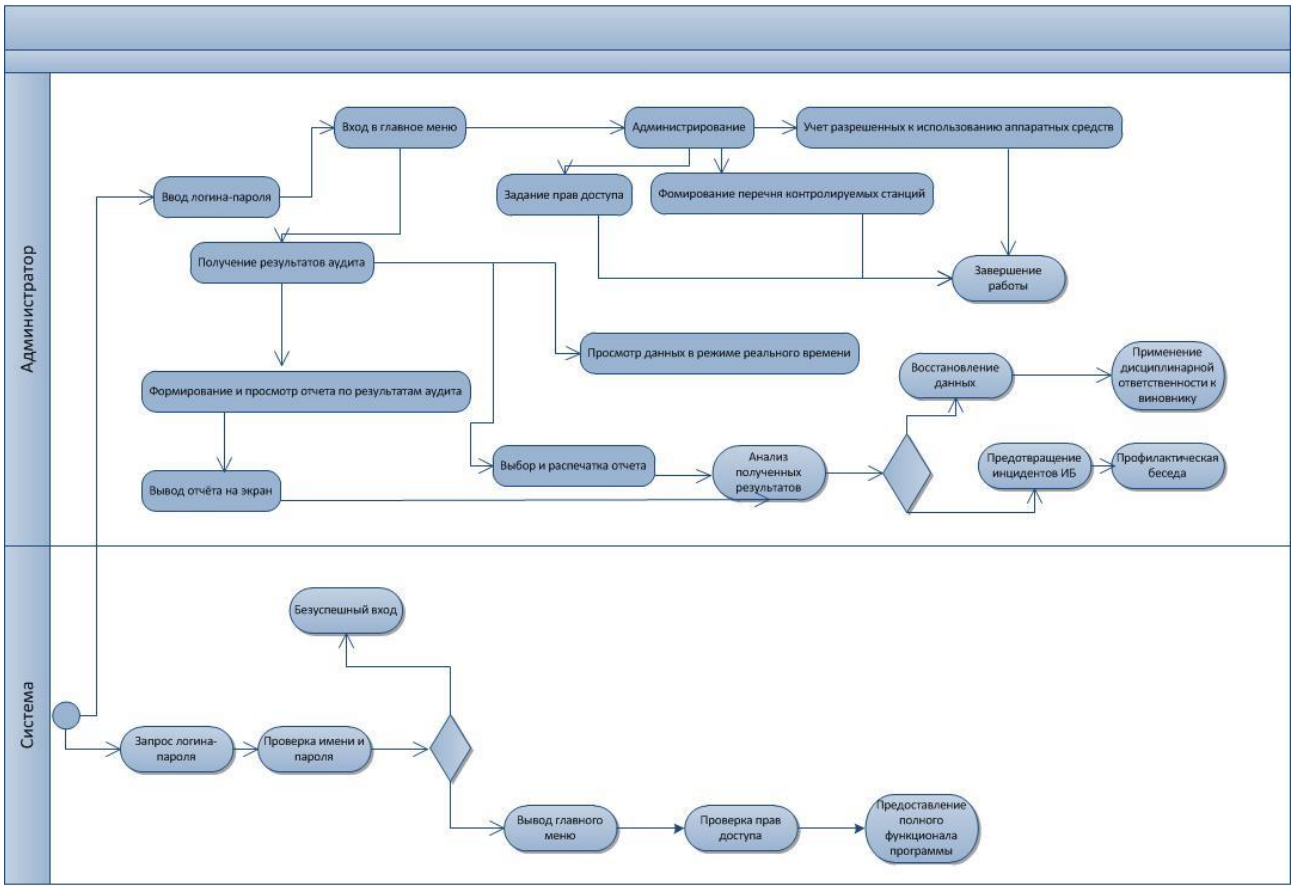

Рисунок 16 – Диаграмма активности

Диаграмма активности UML представленная на рисунке 16, позволяет более детально визуализировать конкретный случай использования. Это поведенческая диаграмма, которая иллюстрирует поток деятельности через систему.

Разработанная диаграмма активности показывает подробное взаимодействие администратора со всеми функциями системы, отражает жизненный цикл системы и предоставляет детальное пояснение к каждой функции.

3.4.5 Диаграмма компонентов

Программный комплекс делится на несколько компонентов. В него

входят:

− база данных base.sql содержит информацию о пользователях и об их действиях в информационных системах;

− доступ к администрированию предоставляется клиентского приложения на рабочую станцию arm.exe, через которое осуществляется установка всех правил информационной безопасности, создание списков и реестров;

− server.exe обрабатывает информацию и сохраняет в базу данных;

− main.db формирует отчёт;

− отчёт.xlsx является конечным файлом, который определяет производительность программы.

Диаграмма компонентов представлена на рисунке 17.

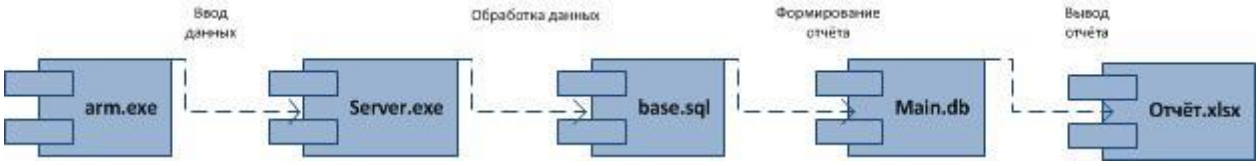

Рисунок 17 – Диаграмма компонентов

3.4.6 Диаграмма развертывания

Диаграмма развертывания – диаграмма, на которой представлены узлы выполнения программных компонентов реального времени, а также процессов и объектов.

Главными элементами диаграммы, представленной на рисунке 18, являются узлы связанные информационными путями. Узлами, представленными на диаграмме выступают устройства (физическое оборудование).

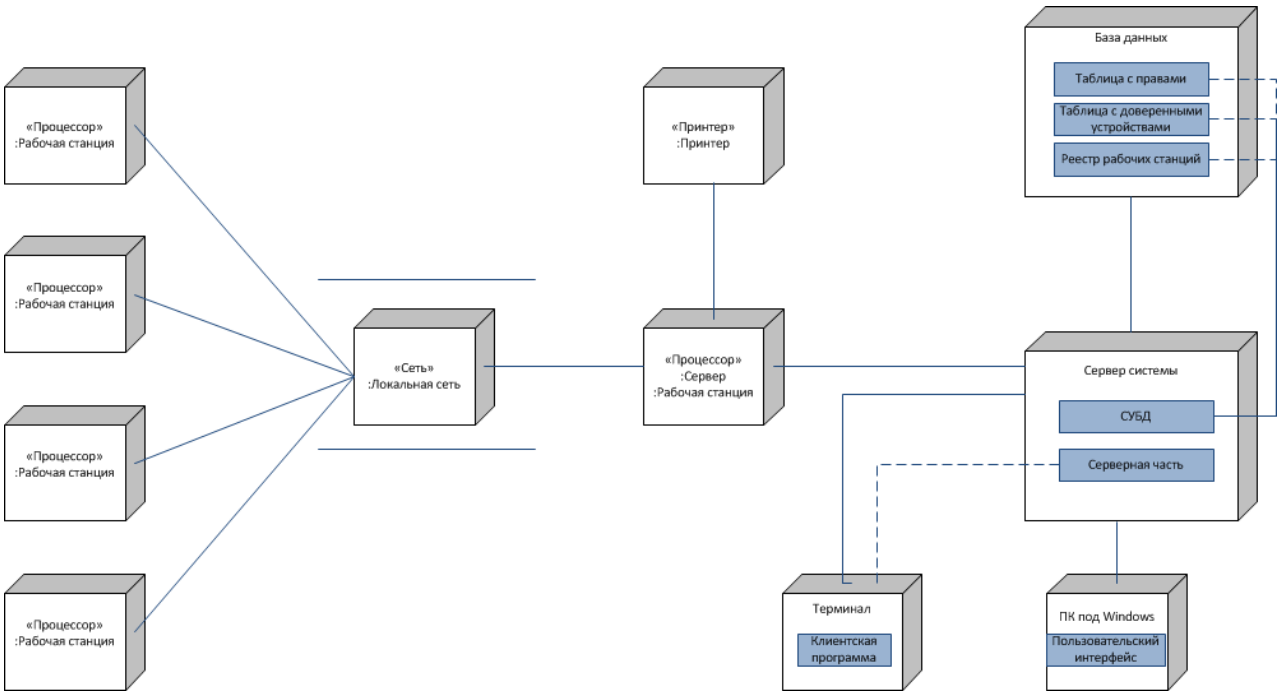

Рисунок 18 – Диаграмма развертывания

3.5 Проектирование функциональных модулей программного обеспечения

Разработка программного обеспечение – это процесс, направленный на создание и поддержание работоспособности, качества и надежности программного обеспечения. Процесс разработки представляет совокупность отдельных этапов, для каждого из которых определены цели и ожидаемые результаты.

Приступая к разработке программного обеспечения, необходимо принять меры для ее упрощения. Для этого программу разрабатывают по частям, которые называются программными модулями. Такой метод создания программ называют модульным программированием.

Модульное программирование основано на понятии модуля – программы или функционально завершенного фрагмента программы.

Составные части характерные для описанной системы автоматизированного аудита и контроля информационных активов предприятия представлены в таблице 6.

Таблица 6 – Составные части алгоритма программного обеспечения

Подсистема сбора данных	Осуществляет с заданной регулярностью опрос объектов, подлежащих мониторингу, для получения исследуемых значений. Может также включать в себя первичный анализ полученных данных с целью, квалификации полученных значений как нормальных, требующих вмешательства оператора либо критических.
Подсистема хранения	Отвечает за накопление, хранение, архивацию данных о результатах проверок.
Подсистема анализа данных	Включает компоненты, производящие исследования данных, накопленных системой, сбор статистики, выработку эталонных значений и сравнение с ними различных состояний наблюдаемой системы.
Подсистема оповещения	Отвечает за уведомление лиц, ответственных за функционирование проверяемых объектов о нештатных ситуациях и иных значимых событиях, возникающих в системе.
Подсистема вывода	Отвечает за представление информации о работе системы и результатов проверок в виде, удобном для восприятия пользователем. Для взаимодействия с конечным пользователем, безусловно, необходим развитый интерфейс, предоставляющий удобную навигацию между различными типами отчетов и сводок о состоянии объектов мониторинга.

Эти подсистемы ориентированы на оперативный мониторинг, направленный на оценку текущей работоспособности и немедленную реакцию на разнообразные внештатные ситуации.

Рисунок 19 – Архитектура системы программного обеспечения

В соответствии с определенными подсистемами и функциями разработано программное обеспечение в среде разработки C++Builder.

3.6 Проектирование базы данных

В качестве базы данных использована СУБД MySQL – самая распространенная полноценная серверная СУБД.

MySQL очень функциональная, свободно распространяемая СУБД, которая успешно работает с различными сайтами и веб приложениями. Обучиться использованию этой СУБД довольно просто, так как на просторах интернета вы легко найдете большее количество информации.

Несмотря на то, что в ней не реализован весь SQL функционал, MySQL предлагает довольно много инструментов для разработки приложений. Так как это серверная СУБД, приложения для доступа к данным, в отличии от SQLite работают со службами MySQL.

Преимущества MySQL:

- простота в работе – установить MySQL довольно просто. Дополнительные приложения, например GUI, позволяет довольно легко работать с БД;
- богатый функционал – MySQL поддерживает большинство функционала SQL;
- Безопасность – большое количество функций обеспечивающих безопасность, которые поддерживается по умолчанию;
- Масштабируемость – MySQL легко работает с большими объемами данных и легко масштабируется;
- Скорость – упрощение некоторых стандартов позволяет MySQL значительно увеличить производительность.

Недостатки MySQL:

- известные ограничения – по задумке в MySQL заложены некоторые ограничения функционала, которые иногда необходимы в особо требовательных приложениях;

− проблемы с надежностью – из-за некоторых способов обработки данных MySQL (связи, транзакции, аудиты) иногда уступает другим системам управления базами данных по надежности;

− медленная разработка – хотя MySQL технически открытое программное обеспечение, существуют жалобы на процесс разработки. Стоит заметить, что существуют другие довольно успешные СУБД созданные на базе MySQL, например MariaDB.

Для связи с базой данных используется DataBase DeskTop 7.0 (DBD), эта программа предназначена для просмотра, создания и редактирования данных и структуры таблицы, а также для запросов к БД. Программа DBD вызывается через главное меню Windows командой Пуск\Borland C++ Builder\Database desktop.DBD включает в себя несколько редакторов:

– редактор структуры таблицы;

– редактор QBE–запроса;

– текстовый редактор SQL-запросов;

– табличный редактор данных.

Доступ к данным организован с помощью двух уровней: набора данных, формируемого на основе непосредственного доступа к физическому хранилищу данных (классы TTable и TQuery), и предоставления источника данных для отображаемых компонент (класс TDataSource). Общее управление сеансом связи приложения с БД определяет класс TSession. C++ Buldera автоматически создает по умолчанию объект класса TSession с именем Session. В программном обеспечении БД при организации обращения к хранимой информации устанавливается соединение с БД – создается компонента класса TDataBase, в данном случае соединение является постоянным.

4 РЕЗУЛЬТАТЫ ФАКТИЧЕСКОГО ТЕСТИРОВАНИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

4.1 Описание интерфейса программного обеспечения

Для работы с данным программным обеспечением при запуске приложения откроется окно авторизации, представленное на рисунке 20, которое предполагает ввод учетных данных.

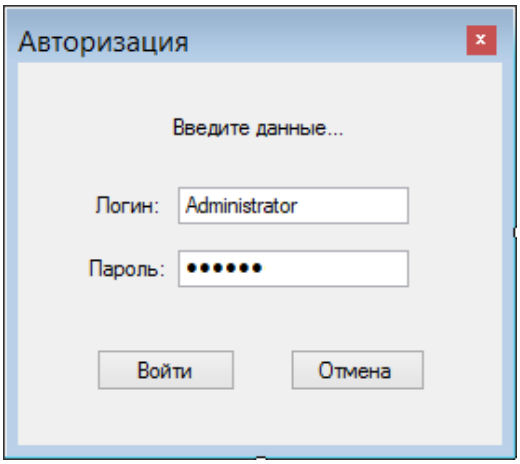

Рисунок 20 – Окно авторизации пользователя

При вводе учетных данных пароль скрыт спецсимволами, данное решение используется для предотвращения несанкционированного доступа к учётным данным пользователя. В случае некорректности ввода учетных данных, пользователь получит сообщение об ошибке и выведет окно авторизации на экран повторно.

Пользовательский интерфейс, представленный на рисунке 21, соответствует заявленным требованиям: прост, интуитивно понятен, информативен.

Составные части интерфейса:

– панель управления – содержит основные команды;

– панель настройки – место для отображения схем основных настроек программы.

– левая область программы предназначена для вывода реестра

контролируемых рабочих станций;

– правая область программы вывод подробную информацию о контролируемой рабочей станции.

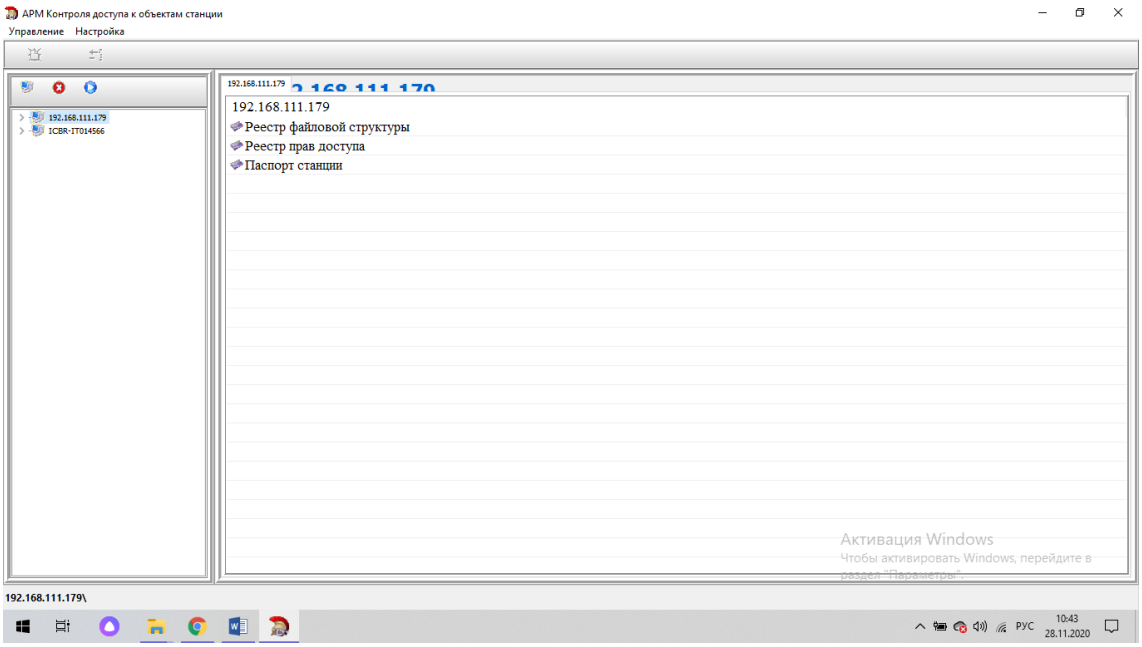

Рисунок 21 – Пользовательский интерфейс программного обеспечения

4.2 Описание основных функций программного обеспечения

Функция предоставления просмотра и изменения реестра прав доступа представлена на рисунке 22.

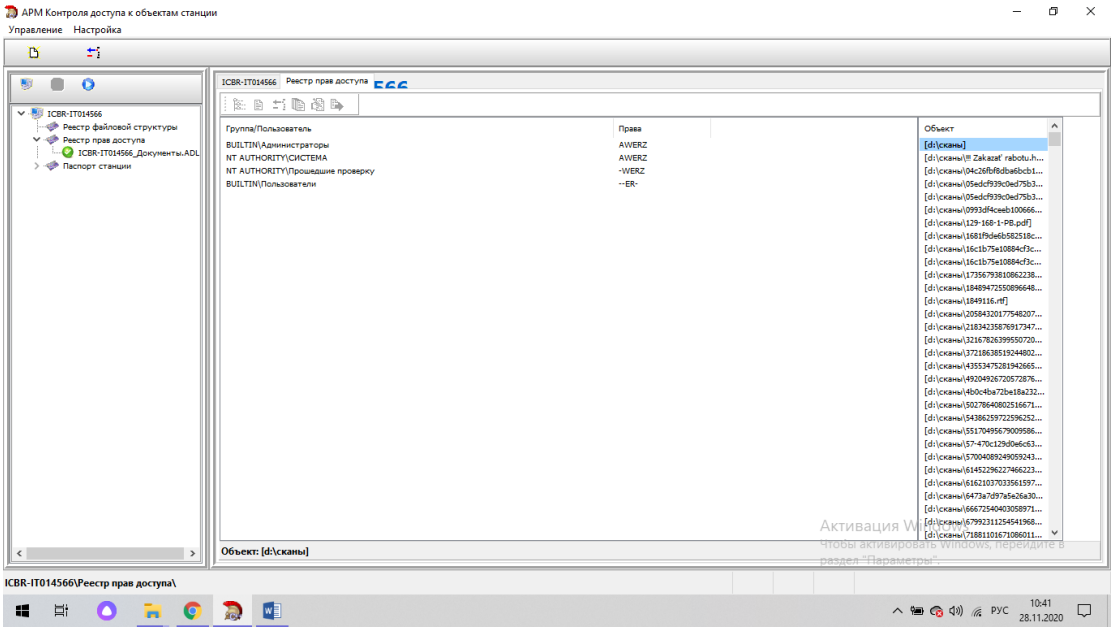

Рисунок 22 – Реестр прав доступа предоставляемых пользователю

Предоставление полных прав к выбранному разделу реестра дает возможность пользователю выполнять любые действия над данным элементом реестра и его подразделами, включая удаление подразделов, создание новых разделов, изменение имен и значений параметров.

После присвоения прав пользователю конкретной рабочей станции в представленном программном обеспечении реализована возможность:

– изменения прав объекта;

– удаление доступа к определенному ресурса, доступ к которому был предоставлен ранее.

Функционал, представленный на рисунке 23, рассчитан на стандартные рабочие ситуации, когда необходимо изменить или закрыть доступ к файловому объекту (кадровые изменения, увольнение).

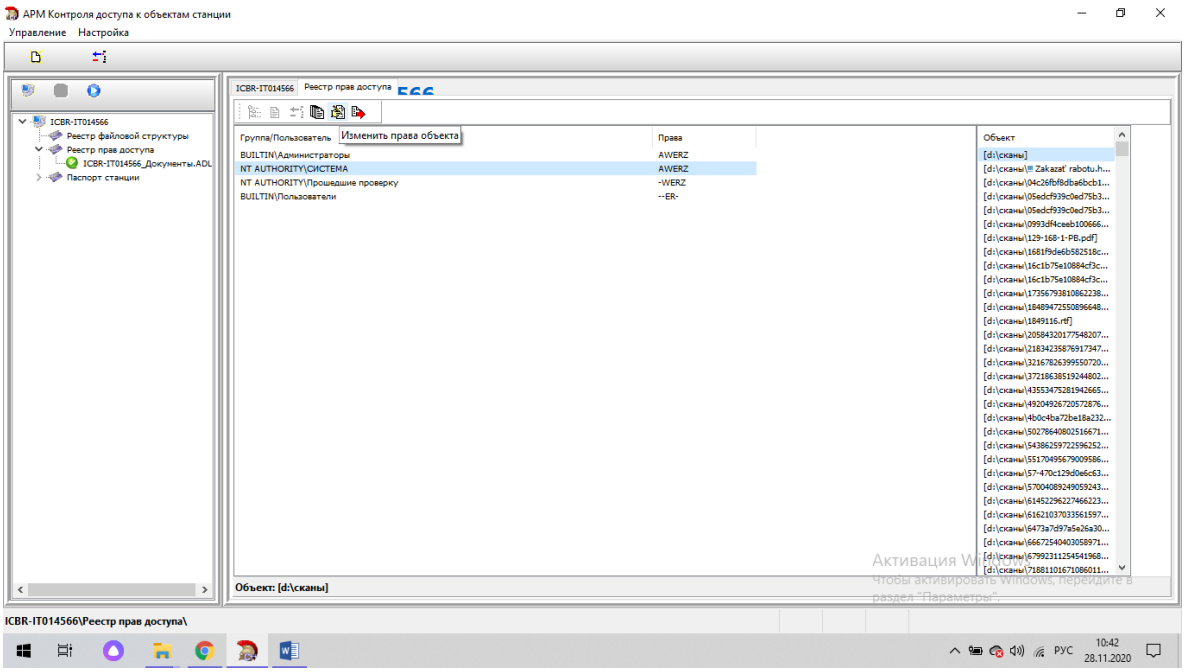

Рисунок 23 – Функция изменения прав доступа к контролируемым объектам

На рисунке 24 и 25 представлена функция «Создания паспорта объекта». Паспорт станции содержит исчерпывающую информацию о контролируемом объекте. Паспорт включает в себя сведения:

– о технических характеристиках;

– о комплектующих устройствах;

– об операционной системе;

– о носителях информации как встроенных, так и съемных;

– о печатных устройствах.

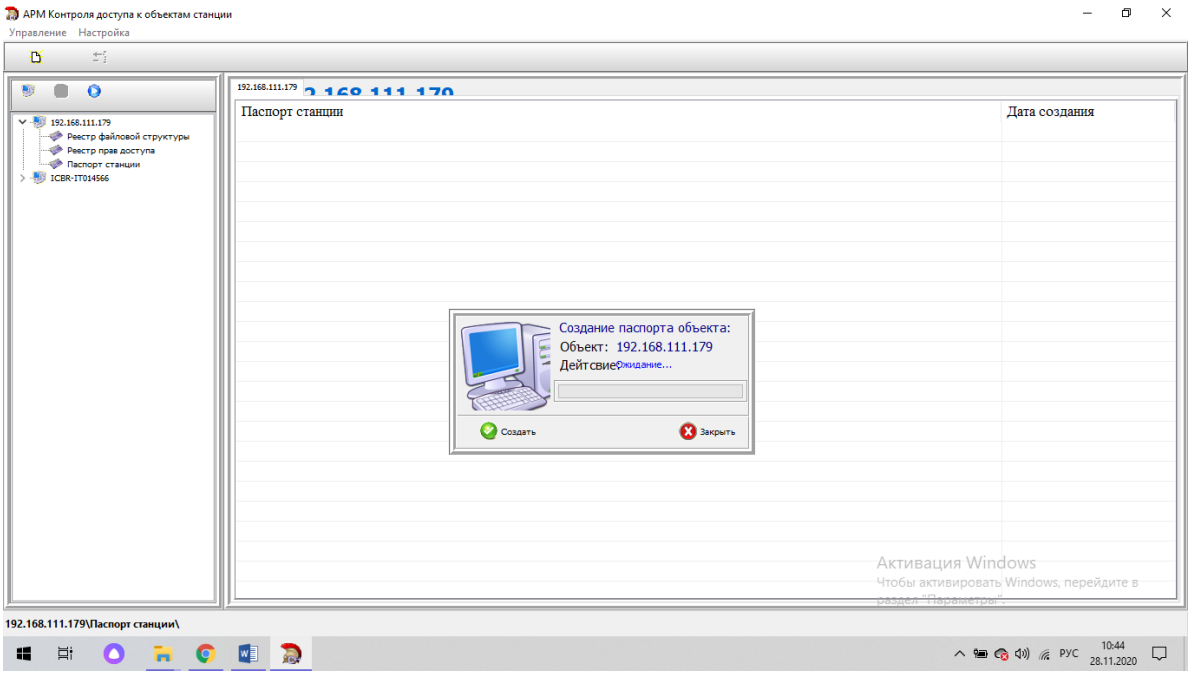

Рисунок 24 – Функция создания паспорта объекта

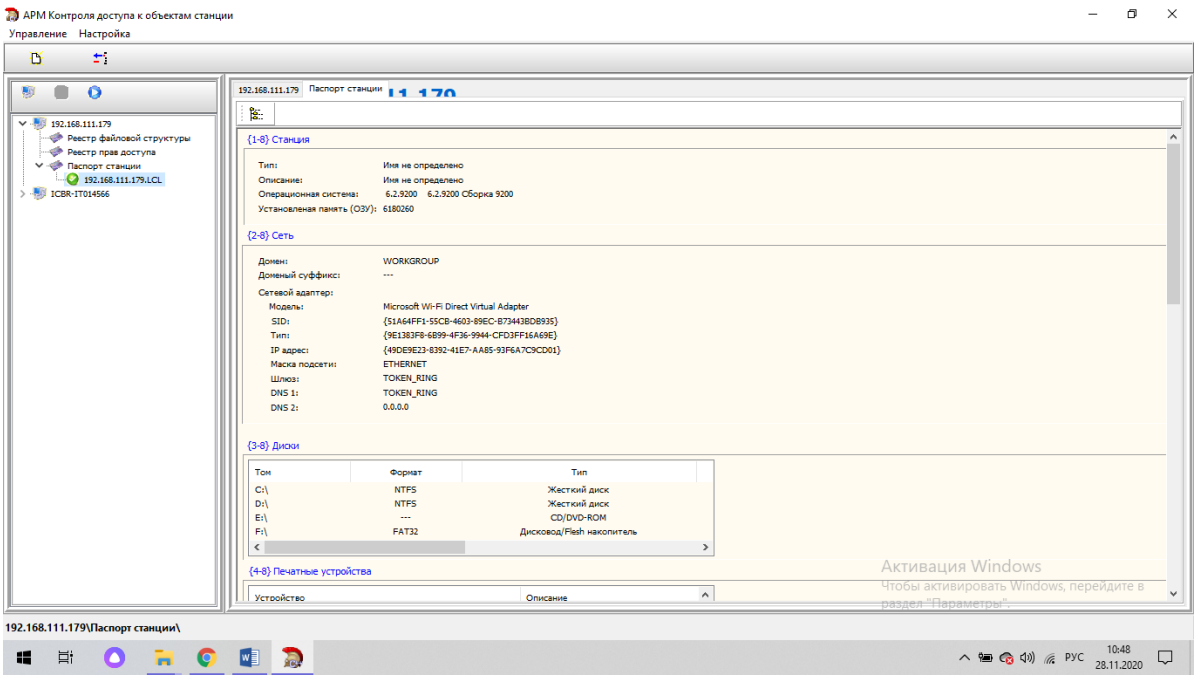

Рисунок 25 – Паспорт объекта

Функция формирования реестра файловой структуры предоставляет возможность разграничения прав доступа к контролируемым объектам. Доступ пользователей к файловому информационному ресурсу предоставляется путем наделения их одним из вариантов полномочий:

– доступ «Только на чтение (Read Only)»;

– доступ «Чтение и запись (Read & Write)».

В подавляющем количестве задач разграничения доступа подобных вариантов полномочий доступа будет достаточно, но при необходимости возможно формирование новых вариантов полномочий, например, «Чтение и запись, кроме удаления (Read & Write without Remove)».

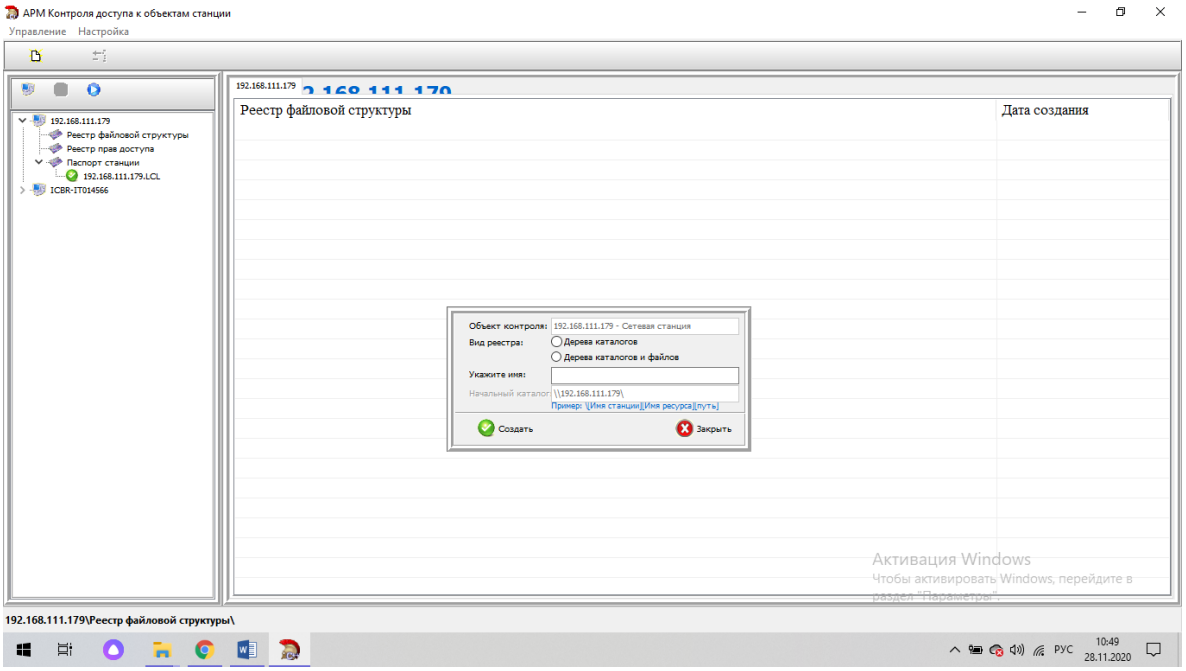

Рисунок 26 – Функция формирования реестра файловой структуры

Данная функция реализована на нескольких процессах:

а) Создание файлового информационного ресурса.

При создании файлового информационного ресурса выполняются следующие действия:

– создаются группы доступа пользователей. Если сервер, на котором размещен файловый информационный ресурс, является членом домена, то

создаются доменные группы.

– на корневой каталог и промежуточные каталоги файлового информационного ресурса назначаются права доступа согласно шаблонам прав доступа;

– в группы доступа пользователей добавляются учетные записи пользователей в соответствии с их полномочиями;

– при необходимости для файлового информационного ресурса создается сетевая папка (shared folder).

б) Предоставление пользователю доступа к файловому информационному ресурсу

– учетная запись пользователя помещается в соответствующую группу доступа пользователя в зависимости от его полномочий.

в) Изменение доступа пользователя к файловому информационному ресурсу;

– учетная запись пользователя перемещается в другую группу доступа пользователей в зависимости от указанных полномочий.

г) Блокирование доступа пользователя к файловому информационному ресурсу;

– учетная запись пользователя удаляется из групп доступа пользователей файлового информационного ресурса. Если работник увольняется, то членство в группах не меняется, а блокируется учетная запись целиком.

д) Создание вложенного файлового информационного ресурса. Расширение доступа;

Данная задача возникает, когда к некоторому каталогу файлового информационного ресурса необходимо предоставить доступ дополнительной группе лиц (расширить доступ). При этом выполняются следующие мероприятия:

– регистрируется вложенный файловый информационный ресурс (согласно процессу а);

– в группы доступа пользователей, вложенного файлового информационного ресурса добавляются группы доступа пользователей вышестоящего составного файлового информационного ресурса.

е) Создание вложенного файлового информационного ресурса. Сужение доступа;

Данная задача возникает, когда к некоторому каталогу файлового информационного ресурса необходимо ограничить доступ и предоставить его только ограниченной группе лиц:

– регистрируется вложенный файловый информационный ресурс (согласно процессу 1);

– в группы доступа пользователей создаваемого информационного ресурса помещаются те учетные записи пользователей, которым требуется предоставить доступ.

ж) Изменение модели предоставления доступа к файловому информационному ресурсу;

В случаях, когда к стандартным вариантам полномочий «Только чтение (Read only)» или «Чтение и запись (Read & Write)» необходимо добавить новые типы полномочий, например, «Чтение и запись, кроме удаления (Read & Write without Remove)» выполняют следующие действия:

– организационными (или техническими, но не связанными с изменением прав доступа к каталогам файловой системы) мерами блокируется доступ пользователей к данному и всем вложенным файловым информационным ресурсам;

– к корневому каталогу файлового информационного ресурса назначаются новые права доступа, при этом заменяются права доступа для всех дочерних объектов (активируется наследие);

– перенастраиваются права доступа для всех вложенных информационных ресурсов;

– настраиваются промежуточные каталоги для данного и вложенных информационных ресурсов.

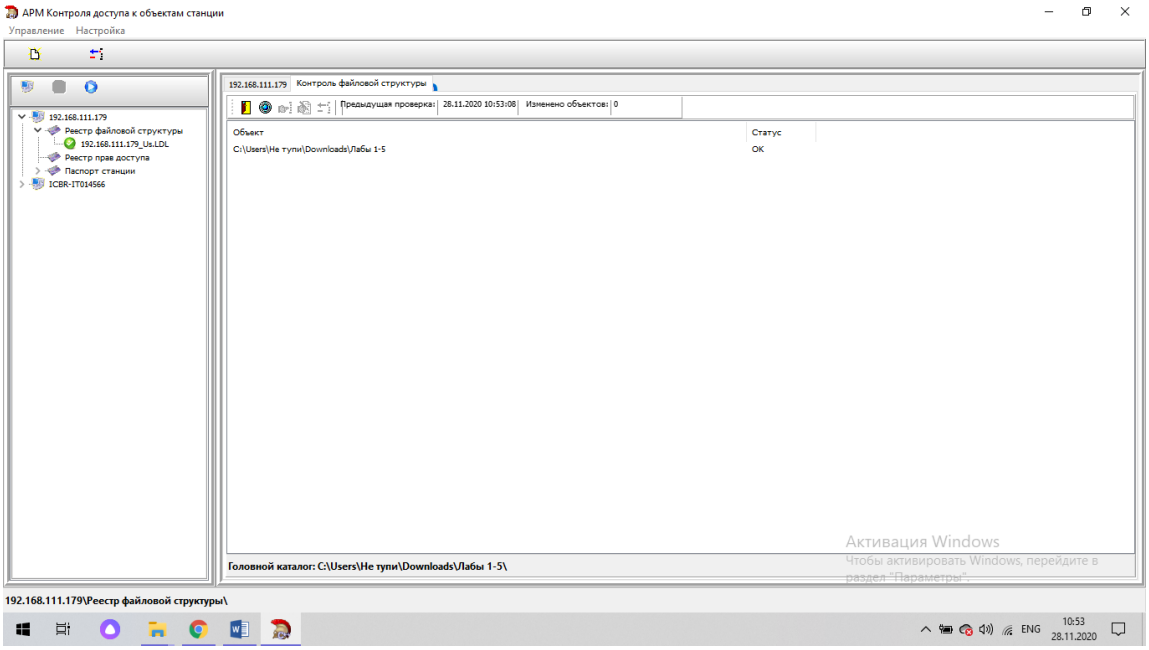

Рисунок 27 – Окно регистрации изменений реестра файловой структуры

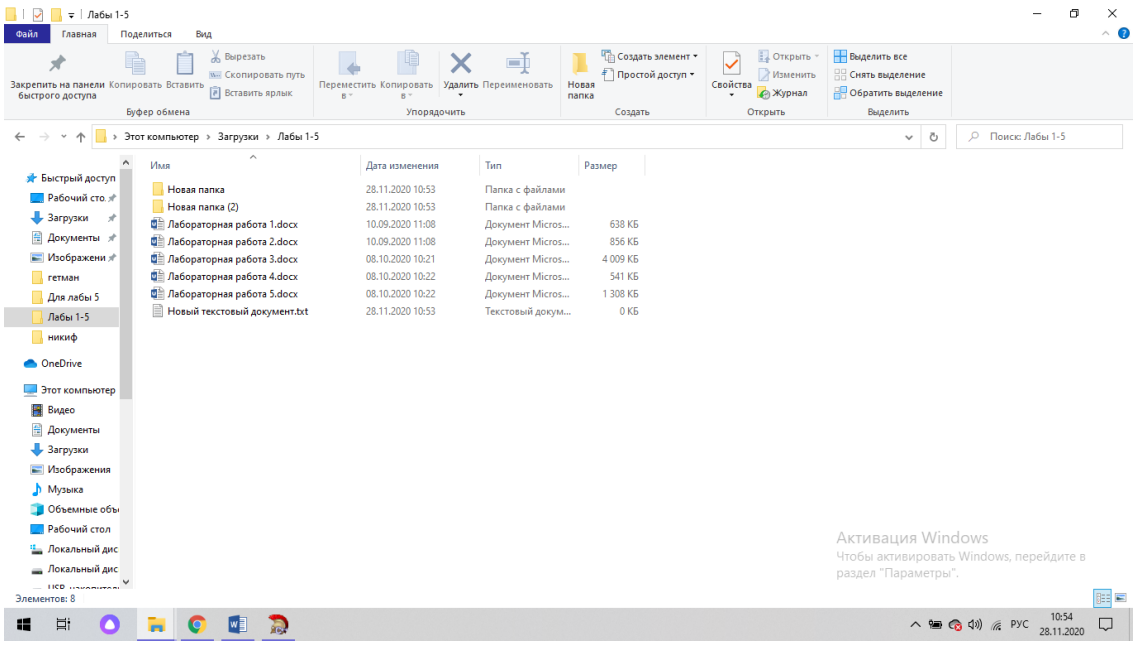

Рисунок 28 – Изменение структуры контролируемого объекта

Факт изменения структуры контролируемого объекта представлено на рисунке 28. В контролируемую программным обеспечением папку был помещен новый файл и переименован имеющийся. На рисунке 29 представлен пример использования функции, регистрации событий, которая предназначена для определения в реальном времени фактов изменения, удаления или иных

действий с объектами доступа.

Программа мгновенно показывает изменения, которые произошли с контролируемым объектом.

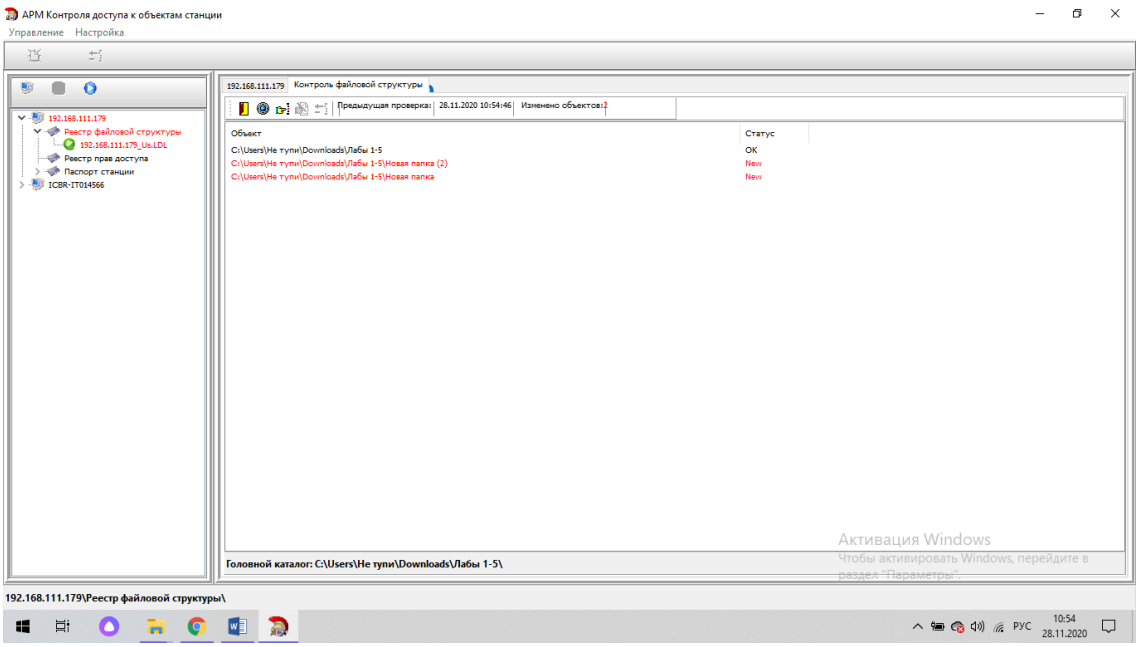

Рисунок 29 – Функция регистрации событий

Весь описанный функционал способствует обнаружению инцидентов информационной безопасности в кратчайшие сроки. Задача администратора информационной безопасности заключается в постоянном аудите рабочих станций, подлежащих контролю, в связи с наличием на них информации ограниченного доступа и персональных данных.

4.3 Анализ достоверности и практической значимости результата

Тестирование программного обеспечения – это процесс его исследования с целью получения информации о качестве. Целью тестирования является выявление дефектов в программного обеспечения. С помощью тестирования нельзя доказать отсутствие дефектов и корректность функционирования анализируемой программы. Тестирование сложных программных продуктов является творческим процессом, не сводящимся к следованию строгим и четким процедурам.

При ручном тестировании тестировщики вручную выполняют тесты, не используя никаких средств автоматизации. Ручное тестирование – самый

низкоуровневый и простой тип тестирования, не требующих большого количества дополнительных знаний.

Автоматизированное тестирование предполагает использование специального программного обеспечения (помимо тестируемого) для контроля выполнения тестов и сравнения ожидаемого фактического результата работы программы. Этот тип тестирования помогает автоматизировать часто повторяющиеся, но необходимые для максимизации тестового покрытия задачи.

В рамках научного исследования выбрано ручное тестирование программного обеспечение на реализацию отдельных видов функций разработанного продукта. Тестирование осуществлялось по двум направлением: авторизация и реагирование на изменение содержимого папок.

Для работы с данным программным обеспечением при запуске приложения открывается окно авторизации, где предложено ввести идентификационные данные. Тестирование функции представленной на рисунке 30, показало, что если ввести неверные идентификационные данные, программа выдаст ошибку.

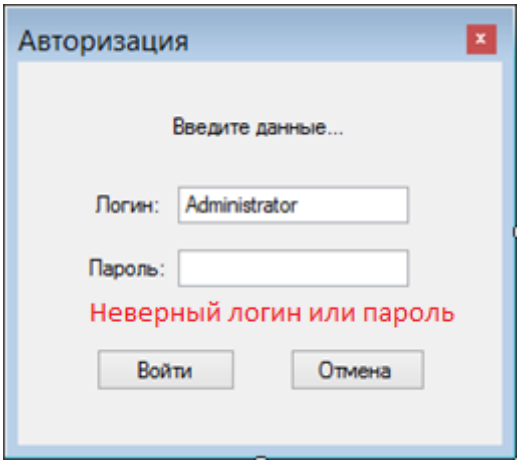

Рисунок 30 – Окно авторизации пользователя

В начале тестирования функции реагирования на изменение содержимого папок, произведен скриншот начального экрана с указанием количества и наименования папок, содержащихся в файловом реестре. Снимок экрана представлен на рисунке 31.

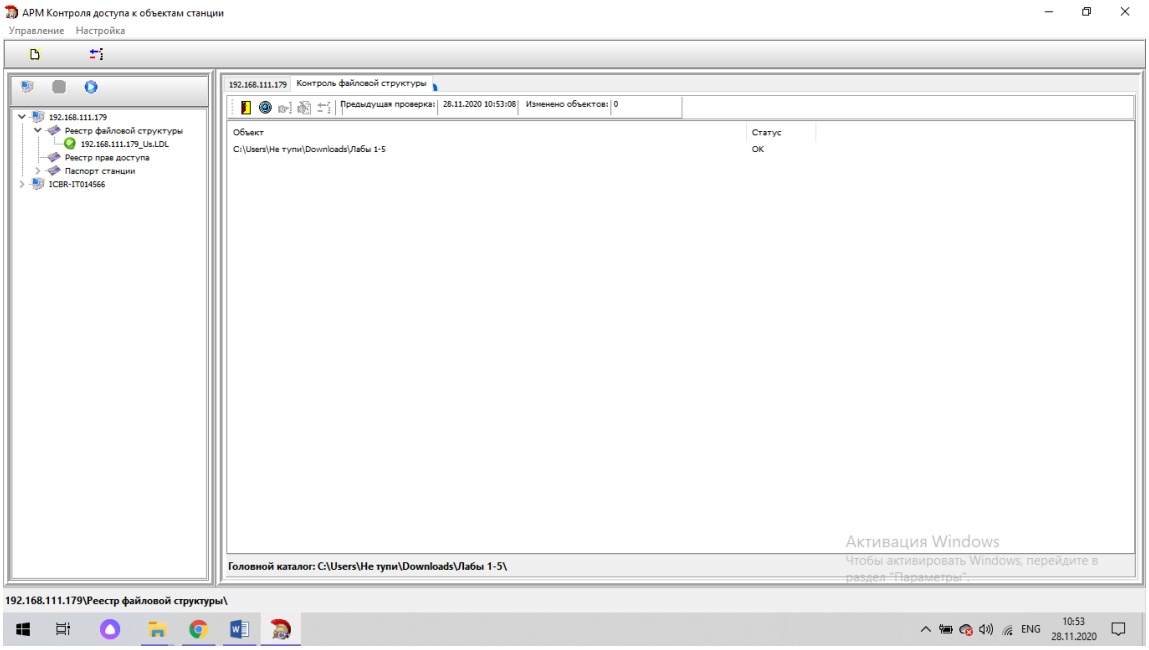

Рисунок 31 – Окно регистрации изменений реестра файловой структуры

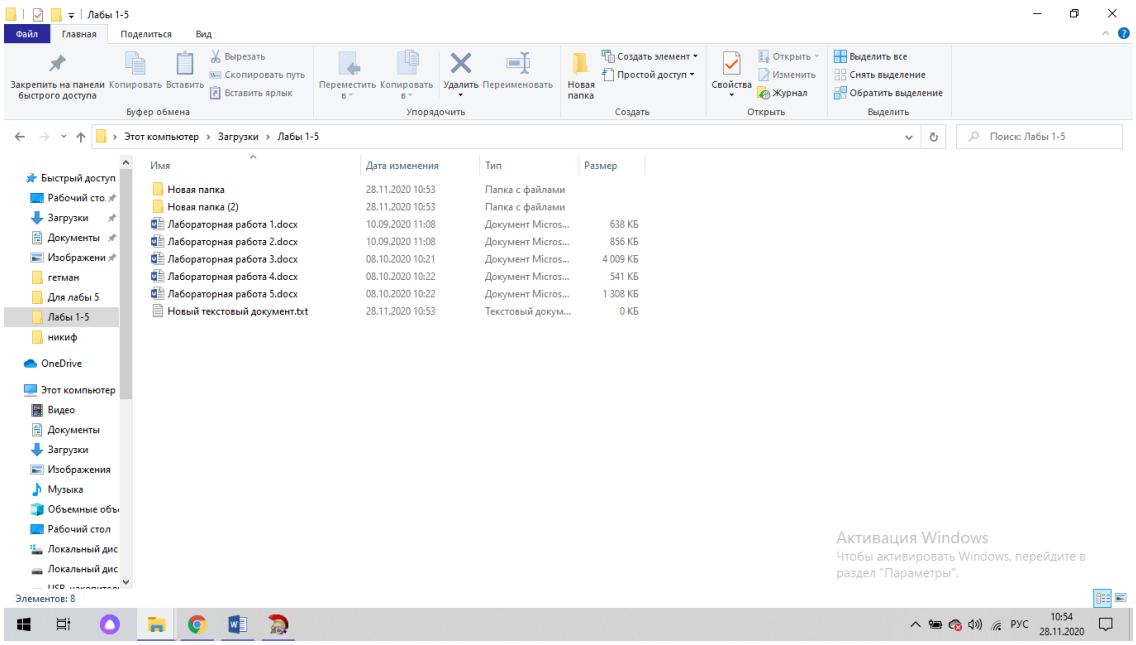

Рисунок 32 – Изменение структуры контролируемого объекта

Далее, произведено изменения структуры контролируемого объекта разработанным программным обеспечением. В контролируемую программным обеспечением папку помещен новый файл и переименован имеющийся. Результаты манипуляций с контролируемым объектом представлены на рисунке 32.

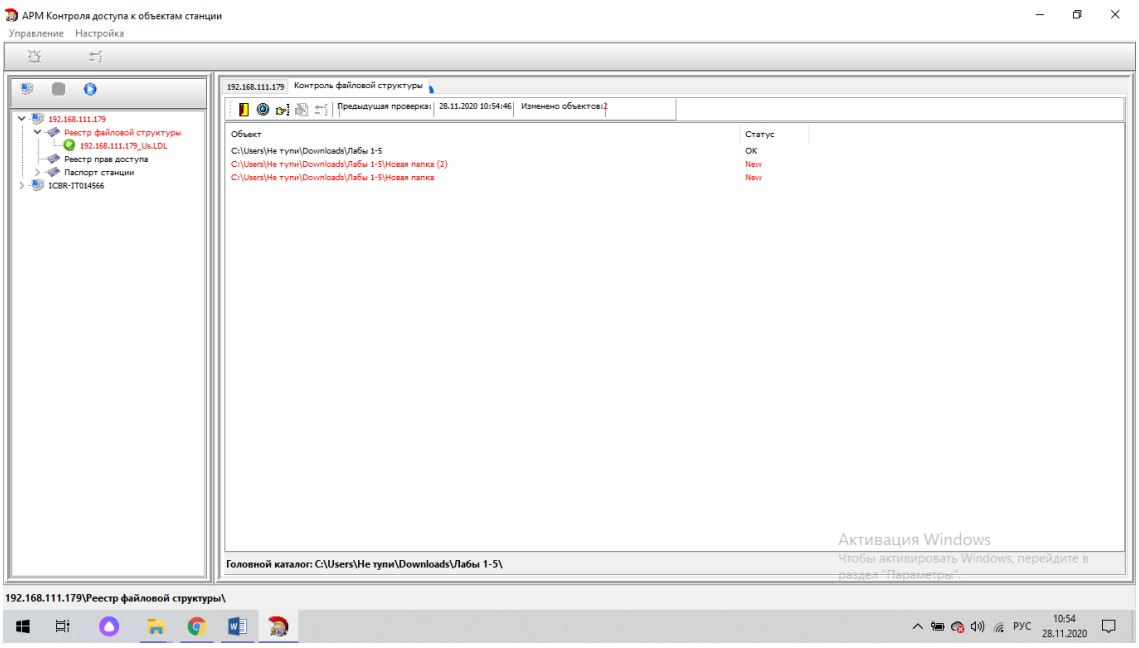

Рисунок 33 – Функция регистрации событий

Факт реагирования программного обеспечения на изменение структуры контролируемого объекта представлен на рисунке 33. Программа мгновенно показывает изменения, которые произошли с контролируемым объектом.

Процесс проверки соответствия заявленных к продукту требований и реально реализованной функциональности показал полное соответствие программного обеспечение заявленным функциям.

ЗАКЛЮЧЕНИЕ

В настоящее время соблюдение требований информационной безопасности одна из важнейших и приоритетных задач любого предприятий. Нарушение требований и стандартов информационной безопасности предприятия способно привести к значительным финансовым потерям, нанесению ущерба репутации предприятия, а также к его полной ликвидации.

Следовательно, обеспечение информационной безопасности любого предприятия зависит от непосредственного контроля за действиями пользователей, а также неукоснительного соблюдение требований информационной безопасности сотрудниками предприятия.

Необходимость оптимизации деятельности территориальных налоговых органов обусловлена не только большим количеством сотрудников предприятия, но и неэффективным распределением ресурса рабочего времени. Совершенствование системы информационной безопасности произведено путем устранения уязвимых мест, а именно внедрением в систему защиты программного обеспечения позволяющего производить автоматизированный аудит и контроль информационных активов предприятия с целью обнаружения несанкционированных действий (обработка, удаление, копирование) информации ограниченного доступа и персональных данных.

Эффективность предотвращения угроз информационной безопасности напрямую зависит от комплексного подхода к решению исследуемой проблемы. Обеспечение необходимого уровня безопасности информационных ресурсов предприятия требует регулярной модернизации системы информационной безопасности, включая усовершенствования нормативно-правовой базы, внедрение новых программных продуктов и проведение обучающих мероприятий для сотрудников.

В ходе научного исследования разработан и реализован проект по оптимизации процессов выявления и предотвращения угроз информационной безопасности территориальных налоговых органов.

В рамках выполнения магистерской диссертации:

- рассмотрены основные цели и задачи обеспечения информационной безопасности;
- исследована нормативно-правовая основа обеспечения информационной безопасности;
- проанализированы существующие методы выявления актуальных угроз информационной безопасности;
- проведен анализ уязвимостей информационной безопасности;
- разработана архитектура и функциональная и теоретико-множественная модель системы мониторинга и аудита;
- описаны алгоритмы функционирования ее модулей и подсистем, выявлено взаимодействие между этими модулями;
- разработан архитектурный проект, включающий в себя UML–диаграммы с подробным описанием;
- разработано программное обеспечение, отвечающее требованиям, заявленным в рамках магистерской диссертации;
- проведен анализ достоверности и практической значимости результата от разработки программного обеспечения.

Таким образом, поставленная цель и задачи достигнуты, что позволило закрепить и пополнить знания в области обеспечения информационной безопасности и разработки программного обеспечения.

Считаю, что разработанное программное обеспечение поможет организациям снизить количество инцидентов информационной безопасности, защитить деятельность организации и противостоять противоправным действиям злоумышленников.

БИБЛИОГРАФИЧЕСКИЕ ССЫЛКИ

1 Баранова, Е.К. Информационная безопасность и защита информации: учебное пособие / Е.К. Баранова, А.В. Бабаш. – М. : Риор, 2018. – 400 с.

2 Блинов, А. М. Информационная безопасность : учеб. пособие. Часть 1 / А. М. Блинов. – СПб. : СПБГУЭФ, 2010. – 96 с.

3 Глинская, Е.В. Информационная безопасность конструкций ЭВМ и систем: учебное пособие / Е.В. Глинская, Н.В. Чичварин. – М. : Инфра–М, 2018. – 160 с.

4 Галатенко, В.А. Основы информационной безопасности : учебное пособие / В.А. Галатенко. – М. : Национальный открытый университет «ИНТУИТ», 2016. – 266 с.

5 Крышкин, О., Настольная книга по внутреннему аудиту: Риски и бизнес–процессы : учебное пособие / О. Крышкин, А. Паблишер. – М. : 2013. – 477 с.

6 Кучеров, И. И. Налоговая тайна в системе мер защиты конфиденциальной информации : учебное пособие / И.И. Кучеров. – М. : Норма, 2015. – 403 с.

7 Пилипенко, В. Ф. Безопасность: теория, парадигма, концепция, культура : словарь–справочник / В. Ф. Пилипенко. – М. : ПЕР СЭ–Пресс, 2005. – 195 с.

8 Семененко, В. А. Информационная безопасность : учебное пособие / В. А. Семененко. – М. : МГИУ, 2004. – 215 с.

9 Стельмашонок Е. В., Васильева. И. Н. Информационная безопасность цифрового пространства / Е.В. Стельмашонок, И.Н. Васильевой. – СПб. : Изд-во СПбГЭУ, 2019. – 155 с.

10 Загорский А. В., Ромашкина Н. П. Угрозы информационной безопасности в кризисах и конфликтах XXI века / А. В. Загорский, Н. П. Ромашкина. – М. : ИМЭМО РАН, 2015. – 151 с.

11 Партыка, Т. Л. Информационная безопасность: учебное пособие / Т. Л. Партыка, И. И. Попов. – Москва: Форум, 2012. – 432 с.

12 Конституция Российской Федерации : офиц. Текст – М. : Приор, 2001. – 32 с.

13 Указ президента Российской Федерации от 5 декабря 2016 г. № 646 «Об утверждении доктрины информационной безопасности Российской Федерации» // Собр. законодательства Российской Федерации. – 2006.

14 Шаньгин, В. Ф. Защита компьютерной информации. Эффективные методы и средства [Электронный ресурс] : учебник / В. Ф. Шаньгин; ДМК Пресс – М., 2010. – Режим доступа: http://www.iprbookshop.ru/7943.– ЭБС «IPRbooks»

15 Шубинский, М.И. Информационная безопасность для работников бюджетной сферы : учебное пособие / М.И. Шубинский. – СПб : НИУ ИТМО, 2012. – 102 с.

16 Беспалов, М.В. Информационное взаимодействие в системе налоговых органов: основные задачи, проблемные точки и перспективы развития / М.В. Беспалов. // Бухгалтер и закон. – 2013. – №51 – С.1 3–17.

17 Вострецова, Е. В. Основы информационной безопасности: учебное пособие / Е. В. Вострецова; Уральский федеральный университет имени первого Президента России Б.Н. Ельцина, Екатеринбург. : 2019 – Режим доступа: https://elar.urfu.ru/bitstream/10995/73899/3/978-5-7996-2677-8_2019.pdf – 11.01.2021

18 Бахтизин, В. В. Технология разработки программного обеспечения: учебное пособие / В. В. Бахтизин, Л. А. Глухова. – Минск : БГУИР, 2010. – 267 с.

19 Перл И. А., Калёнова О. В. Введение в методологию программной инженерии : учебное пособие / И. А. Перл, О. В. Калёнова; Университет ИТМО, СПб. : 2019 – Режим доступа: https://books.ifmo.ru/file/pdf/2491.pdf – 16.01.2021

20 Ехлаков, Ю. П., Управление программными проектами : учебное

пособие / Ю. П. Ехлаков; Томский государственный университет систем управления и радиоэлектроники, Томск. : 2014 – Режим доступа: https://aoi.tusur.ru/upload/methodical_materials/Upr_progr__proektami_uchebnik_file__504_8555.pdf – 15.02.2021

21 Советов, Б. Я. Моделирование систем. Практикум / Б.Я. Советов, С.А. Яковлев. – М. : Юрайт, 2012. – 296 с.

22 Гудов, А. М. Технология разработки программного обеспечения : учебное пособие / А. М. Гудов, С. Ю. Завозкин, С. Н. Трофимов. – Кемерово : Кемеровский государственный университет, 2009. – 138 с.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1 Аллен, Э. Типичные ошибки проектирования / Э. Аллен. – СПб : Питер, 2003. – 224 с.

2 Аронов, А. В., Кашин, В. А. Налоговая политика и налоговое администрирование: учебное пособие / А. В. Аронов, В. А. Кашин. – М.: Экономист, 2006. – 188 с.

3 Артемов, А. В. Информационная безопасность : учебное пособие / А. В. Артемов. – Орёл: Литагент «МАБИВ», 2014. – 51 с.

4 Баранова, Е. К. Информационная безопасность и защита информации: учебное пособие / Е. К. Баранова, А. В. Бабаш. – М. : Риор, 2018. – 400 с.

5 Бармен, Скотт. Разработка правил информационной безопасности : учебное пособие / Скотт Бармен. – Вильямс, 2002. – 208 с.

6 Бахтизин, В. В. Технология разработки программного обеспечения: учебное пособие / В. В. Бахтизин, Л. А. Глухова. – Минск : БГУИР, 2010. – 267 с.

7 Блинов, А. М. Информационная безопасность : учеб. пособие. Часть 1 / А. М. Блинов. – СПб. : СПБГУЭФ, 2010. – 96 с.

8 Буч Г., Рамбо Д., Джекобсон А. Язык UML Руководство пользователя / Г. Буч, Д. Рамбо, А. Джекобсон. – СПб : Издательство «Питер», 2010. – 432 с.

9 Галаган, Т. А. Технология разработки программного обеспечения: сборник учебно-методических материалов для направления подготовки 09.04.04 Программная инженерия : учебно-методический материал / Т. А. Галаган. – Благовещенск : Амурский государственный университет, 2018. – 51 с.

10 Галатенко, В. А. Основы информационной безопасности : учебное пособие / В.А. Галатенко. – М. : Национальный открытый университет «ИНТУИТ», 2016. – 266 с.

11 Галицкий, А. В., Рябко, С. Д., Шаньгин, В. Ф. Защита информации в сети – анализ технологий и синтез решений : учебное пособие / А. В. Галицкий,

С. Д. Рябко, В. Ф. Шаньгин. – М. : ДМК Пресс, 2004. – 615 с.

12 Гатчин, Ю. А. Теория информационной безопасности и методология защиты информации : учеб. пособие / Ю. А. Гатчин, В. В. Сухостат. – СПб. : ИТМО, 2010. – 98 с.

13 Глинская, Е. В. Информационная безопасность конструкций ЭВМ и систем: учебное пособие / Е. В. Глинская, Н. В. Чичварин. – М. : Инфра-М, 2018. – 160 с.

14 Голицына, О. Л., Программное обеспечение : учебное пособие / О. Л. Голицына. – М. : Форум, 2013. – 448 с.

15 Гришина, Н. В. Информационная безопасность предприятия: учебное пособие / Н. В. Гришина. – М. : Форум, 2018. – 118 с.

16 Гудов, А. М. Технология разработки программного обеспечения : учебное пособие / А. М. Гудов, С. Ю. Завозкин, С. Н. Трофимов. – Кемерово : Кемеровский государственный университет, 2009. – 138 с.

17 Громов, Ю. Ю. Представление знаний в информационных системах : учебное пособие / Ю. Ю. Громов. – Тамбов : Тамбовский государственный технический университет, ЭБС АСВ, 2012. – 169 с.

18 Затонский, А. В. Программирование и основы алгоритмизации / А. В. Затонский. – М. : Дрофа, 2014. – 176 с.

19 Крат, Ю. Г. Основы информационной безопасности : учеб. пособие / Ю. Г. Крат, И. Г. Шрамкова. – Хабаровск : Изд–во ДВГУПС, 2008. –112 с.

20 Крышкин, О., Настольная книга по внутреннему аудиту: Риски и бизнес-процессы : учебное пособие / О. Крышкин, А. Паблишер. – М. : 2013. – 477 с.

21 Кучеров, И. И. Налоговая тайна в системе мер защиты конфиденциальной информации : учебное пособие / И. И. Кучеров. – М. : Норма, 2015. – 403 с.

22 Либерти, Д. Язык программирования C# // Программирование на C# : учебное пособие / Д. Либерти. – СПб :Символ–Плюс, 2003. – 688 с.

23 Макаренко, С. И. Информационная безопасность : учебное пособие

для студентов вузов / С. И. Макаренко. – Ставрополь : СФ МГГУ им. М. А. Шолохова, 2009. – 372 с.

24 Мартин, Р. Чистый код. Создание, анализ и рефакторинг. Библиотека программиста / Р. Мартин. – СПб : Питер, 2014. – 464 с.

25 Мещеряков, С. В. Эффективные технологии создания информационных систем / С. В. Мещеряков, В. М. Иванов. – М. : Политехника, 2005. – 312 с.

26 Панюкова, Т. А. Проектирование программных средств / Т. А. Панюкова. – М. : Гостехиздат, 2012. – 364 с.

27 Партыка, Т. Л. Информационная безопасность: учебное пособие / Т. Л. Партыка, И. И. Попов. – М.: Форум, 2012. – 432 с.

28 Петров, С. В. Информационная безопасность: учебное пособие / С. В. Петров, И. П. Слинькова, В. В. Гафнер. – Москва: АРТА, 2012. – 296 с.

29 Петренко, С. А. Аудит безопасности Intranet : учебное пособие / С. А. Петренко, А. А. Петренко. – ДМК Пресс, 2002. – 406 с.

30 Пилипенко, В. Ф. Безопасность: теория, парадигма, концепция, культура : словарь–справочник / В. Ф. Пилипенко. – М. : ПЕР СЭ–Пресс, 2005. – 195 с.

31 Розенберг Д., Скотт К. Применение объектного моделирования с использованием UML и анализ прецедентов : учебное пособие / Д. Розенберг, К. Скотт. – Москва: ДМК Пресс, 2002. – 158 с.

32 Семененко, В. А. Информационная безопасность : учебное пособие / В. А. Семененко. – М. : МГИУ, 2004. – 215 с.

33 Советов, Б. Я. Моделирование систем. Практикум / Б. Я. Советов, С. А. Яковлев. – М. : Юрайт, 2012. – 296 с.

34 Снытников, А. А. Лицензирование и сертификация в области защиты информации : учебное пособие / А. А. Снытников. – М : Гелиос АРВ, 2003. – 192 с.

25 Шилдт, Г. Полный справочник по C# = C#: The Complete Reference : учебное пособие / Г. Шилдт. – М. :Издательский дом «Вильямс», 2004. – 752 с.

36 Шубинский, М. И. Информационная безопасность для работников бюджетной сферы : учебное пособие / М. И. Шубинский. – СПб : НИУ ИТМО, 2012. – 102 с.

37 Ярочкин, В. И. Информационная безопасность: учебник для студентов : учебное пособие / В. И. Ярочкин. – М. : Гаудеамус, 2004. – 544 с.

38 Аверченков, В. И., Аудит информационной безопасности органов исполнительной власти [Электронный ресурс] : учебное пособие / В. И. Аверченков ; Брянский государственный технический университет – Брянск. : 2012. – Режим доступа: http://www.iprbookshop.ru/6992.html. – ЭБС «IPRbooks» – 25.02.2021

39 Аверченков, В. И. Аудит информационной безопасности [Электронный ресурс] : учебное пособие для вузов / В. И. Аверченков ; Брянский государственный технический университет – Брянск. : 2012 – Режим доступа: http://www.iprbookshop.ru/6991.html – 18.09.2020

40 Аверченков, В. И. Основы математического моделирования технических систем [Электронный ресурс] : учебное пособие / В. И. Аверченков, В. П. Федоров, М. Л. Хейфец ; Брянский государственный технический университет – Брянск. : 2012 – Режим доступа: http://www.iprbookshop.ru/7003.html. – ЭБС «IPRbooks» – 23.12.2020

41 Шаньгин, В. Ф. Защита компьютерной информации. Эффективные методы и средства [Электронный ресурс] : учебник / В. Ф. Шаньгин; ДМК Пресс – М., 2010. – Режим доступа: http://www.iprbookshop.ru/7943.– ЭБС «IPRbooks»

42 ГОСТ Р ИСО/МЭК 12207–2010, Информационная технология. Системная и программная инженерия. Процессы жизненного цикла программных средств, 2010 г. – 105 с.

43 Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных // ФСТЭК. – 2008.

44 Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных // ФСТЭК. – 2008.

45 Постановление правительства от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» // Собр. законодательства Российской Федерации. – 2012.

46 Приказ ФСТЭК от 18 февраля 2013 г. № 21 в ред. Приказ ФСТЭК от 14.05.2020 № 68 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационной системе персональных данных» // ФСТЭК. – 2013.

47 Федеральный закон от 27 июля 2006 г. №149-ФЗ в ред. ФЗ ред. от 09.03.2021 № 39-ФЗ «Об информации, информационных технологиях и защите информации» // Собр. законодательства Российской Федерации. – 2006.

48 Федеральный закон от 27 июля 2006 г. №152-ФЗ (в ред. ФЗ ред. от 30.12.2020 № 519-ФЗ) «О персональных данных» // Собр. законодательства Российской Федерации. – 2006.

49 Федеральный закон от 30 декабря 2008 г. № 307-ФЗ в ред. ФЗ ред. от 09.03.2021 № 41-ФЗ «Об аудиторской деятельности» // Собр. законодательства Российской Федерации. – 2008.

50 Беспалов, М. В. Информационное взаимодействие в системе налоговых органов: основные задачи, проблемные точки и перспективы развития / М. В. Беспалов. // Бухгалтер и закон. – 2013. – № 51 – С. 13-17.

51 Котина, Г. А., Карпеева, Н. М. Функции налогового администрирования в проекте модернизации ФНС России. Планы и реальность / Г. А. Котина, Н. М. Карпеева // Финансы. – 2015. – № 30 – С. 26-29.

52 Ложкова А. А. Защита биометрических персональных данных в медицинских информационных системах / А. А. Ложкова // Материалы XIV Международной научной конференции «САМ 2020». – 2020. – С.69-72.

53 Манык, П. В. Правовые основы безопасности виртуальной среды / П. В. Манык // Журнал Information Security. Информационная безопасность. – 2016. – № 2(35). – С. 33.

54 Новицкая, Е. А., Зубарева, Е. Г. Информационные технологии, их развитие в сфере налогообложения и переход налоговых органов на АИС «Налог–3» / Е. А. Новицкая, Е. Г. Зубарева. // Научный альманах, 2015. – № 25. – С. 160-163.

55 Самохвалова С. Г., Ложкова А. А. Аудит информационной безопасности на предприятии / С. Г. Самохвалова, А. А. Ложкова // Молодежь XXI века: Шаг в будущее, 2020. – С. 120-121.

56 Самохвалова С. Г., Ложкова А. А. Комплексная система защиты информации в организации / С. Г. Самохвалова, А. А. Ложкова // Тенденции развития науки и образования, 2021. – С. 79-82.

57 Селифанов, В. В., Слонкина, И. С., Юракова, Я.В. Определение актуальных угроз безопасности информации в государственных информационных системах, используя Банк данных угроз / В.В. Селифанов, И. С. Слонкина, Я. В. Юракова. // Наука. Технологии. Инновации: сборник научных трудов в 9 частях. – 2016. – С. 69-71.

58 Стрельцов, А.А. Содержание понятия «обеспечение информационной безопасности» / А.А. Стрельцов. – М. : Информационное общество № 4, 2015. – 12 с.

59 Цветкова, О. Л., Айдинян, А. Р. Интеллектуальная система оценки информационной безопасности предприятия от внутренних угроз / О. Л. Цветкова, А. Р. Айдинян. // Вестник компьютерных и информационных технологий, 2014. – № 8(122). – С. 48-53.