Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«Уральский федеральный университет
имени первого Президента России Б.Н. Ельцина»

Институт экономики и управления

Кафедра анализа систем и принятия решений

ДОПУСТИТЬ К ЗАЩИТЕ ПЕРЕД ГЭК

Зав. кафедрой АСиПР

_____Медведева М.А._____
(подпись) (Ф.И.О.)

«05» июня 2020 г.

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА (МАГИСТЕРСКАЯ ДИССЕРТАЦИЯ)

Методика предотвращения угроз информационной безопасности на предприятии

Научный руководитель: Ермаков Д.Г.

к.ф.-м.н.

Научный руководитель: Турыгина В.Ф.

Консультант: Толмачев А.В.

старший преподаватель

Нормоконтролер: Медведева М.А.

зав. кафедрой, к.ф.-м.н., доцент

Студент группы ЭУМ-280001, Шушарина Е.Е.

Екатеринбург
2020

РЕФЕРАТ

Тема магистерской диссертации:

Методика предотвращения угроз информационной безопасности на предприятии

Магистерская диссертация выполнена на 101 страницах, содержит 14 таблиц, 23 рисунка, 62 использованных источников.

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.

Цель магистерской работы: внедрение комплексной методики выявления и предотвращения угроз информационной безопасности с целью совершенствования системы защиты информации.

Для достижения поставленной 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;
- разработать комплексный план мероприятий, направленных на сокращение угроз информационной безопасности;
- построить модели AS-IS и TO-BE;
- выполнить адаптацию и внедрение методики;

- оценить результаты внедрения;
- выполнить расчет экономической эффективности внедрения.

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

Основные пункты научной/методологической новизны диссертации:

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

Данные работы несут теоретических характер и не могут быть применимы для минимизации угроз информационной безопасности в процессе работы территориальных налоговых органов.

Практическая значимость исследования:

В ходе создания данного проекта были автоматизированы основные этапы процесса выявления нарушений информационной безопасности.

Практическая значимость данного проекта заключается в:

- усовершенствовании методики предотвращения угроз информационной безопасности в процессе работы территориальных налоговых органов;
- автоматизация основных процессов выявления угроз информационной безопасности.

Методика предотвращения угроз информационной безопасности целесообразна для эксплуатации на практике, и будет способствовать не только рациональному расходу рабочего времени, но и поддержанию состояния информационной безопасности на объекте информатизации. Реализация проекта направлена на усиления контроля информационной безопасности.

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: внедрение комплексной методики выявления и предотвращения угроз информационной безопасности с целью совершенствования системы защиты информации.

Для достижения поставленной 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;
- разработать комплексный план мероприятий, направленных на сокращение угроз информационной безопасности;
- построить модели AS-IS и TO-BE;
- выполнить адаптацию и внедрение методики;
- оценить результаты внедрения;
- выполнить расчет экономической эффективности внедрения.

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

Используемые методы исследования:

- анализ литературы и нормативно-правовых документов по теме исследования;
- сравнение;
- моделирование (получение информации о предмете через созданную модель);
- измерение (получение количественных данных);
- изучение и обобщение сведений.

Степень разработанности темы:

Проблеме предотвращения угроз информационной безопасности федеральных органов исполнительной власти посвящены работы таких авторов, как Коровяковский Д.Г., Кириллова О.С., Терещенко Л.К., Тиунов О.И., Соколов Д.В., Джафарова З.К.

Работы данных авторов содержат фундаментальные знания об информационной безопасности органов исполнительной власти, раскрывают основные понятия, определения, функции, рассматривают нормативно-правовую базу, которая регламентирует деятельность налоговых органов в сфере обеспечения информационной безопасности.

Данные работы несут теоретических характер и не могут быть применимы для минимизации угроз информационной безопасности в процессе работы территориальных налоговых органов.

Основные пункты научной/методологической новизны диссертации:

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

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

В ходе работы были построены модели исследуемых бизнес-процессов и разработана новая методика выявления и предотвращения угроз информационной безопасности.

Практическая значимость исследования:

В ходе создания данного проекта были автоматизированы основные этапы процесса выявления нарушений информационной безопасности.

Практическая значимость данного проекта заключается в:

- усовершенствовании методики предотвращения угроз информационной безопасности в процессе работы территориальных налоговых органов;
- автоматизация основных процессов выявления угроз информационной безопасности.

Эмпирическая база:

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

Структура магистерской диссертации состоит из введения, трех разделов, заключения и списка использованных источников.

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

Во второй главе подробно рассмотрена нормативная база, обеспечивающая информационную безопасность, были выявлены основные недостатки действующих методов выявления угроз информационной безопасности на предприятии, а также был произведен обзор наиболее актуальных угроз информационной безопасности предприятия и произведен расчет уровня их возможной реализации.

В третьей главе представлена характеристика Федеральной налоговой службы, была проведена разработка комплексного плана мероприятий, направленного на сокращение угроз информационной безопасности. Построены модели AS-IS и TO-BE. Разработан план внедрения программного продукта «БЛОКХОСТ-СЕТЬ 2.0». Сформулированы основные результаты внедрения методики, а также проведено экономическое обоснование проекта.

В процессе выполнения работы был использован инструментарий MS Word, MS Project, MS Excel, MS Visio, MS Power Point.

1 ТЕОРЕТИЧЕСКИЕ АСПЕКТЫ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1.1 Понятие и сущность 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, способствующем 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 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. Неопределенное понимание самой сущности информационной безопасности, в свою очередь, может спровоцировать неправильное направление в развитии и разработке средств защиты информации, в том числе программные обеспечения, аппаратные или технические средства защиты, а также структуры по защите информации.

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 также нанести ущерб также его функциональной деятельности или самим свойствам объекта защиты [2].

Официальное определение информационной безопасности представлено в Доктрине информационной безопасности от 05.12.16 [3]. Для более наглядного представления об основных составляющих официального определения информационной безопасности представлена системообразующая схема на рисунке 1.

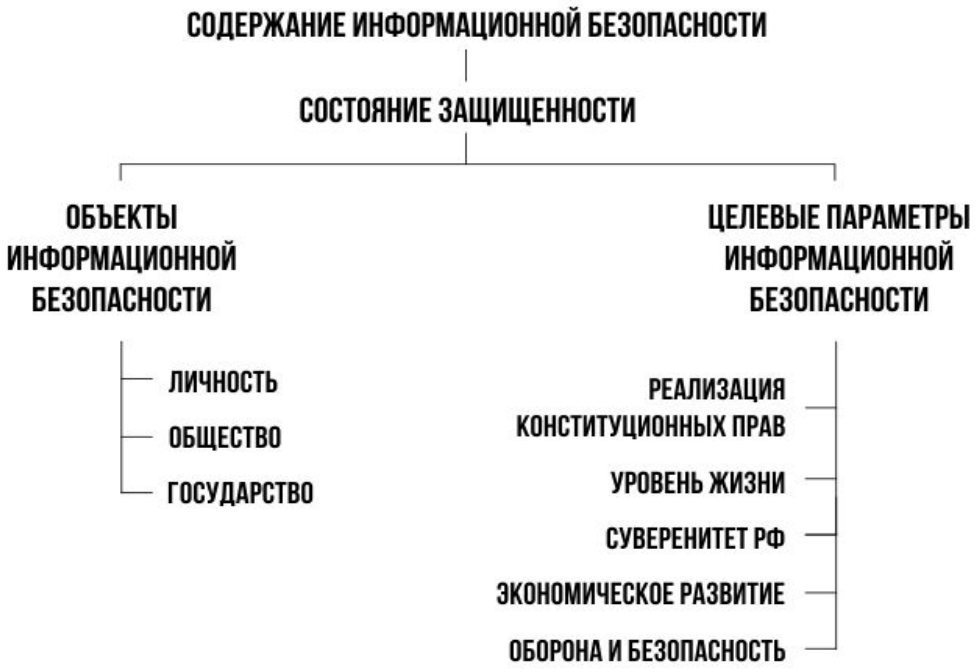


Рисунок 1 – Основные составляющие определения информационной безопасности[1]

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. 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

[1] Составлено автором по: [44]

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 [10]. Исходя из вышесказанного, следует понимать, что защита персональных данных обоснованно следует отожествлять с защитой конфиденциальной информации и представлять из себя социальную ценность [11]. 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 можно определить как разработку и реализацию 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 можно определить как 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. Состояние информационной защищенности может быть обеспечено как в технической способности объекта защиты противодействовать несанкционированному воздействию из вне, так и результатом проведения мероприятий, направленных на поддержание безопасного состояния информационной среды.

1.2 Цели и задачи обеспечения информационной безопасности

Генеральной 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 основные направления для достижения данной цели: стабильное поддержание конфиденциальности защищенной информации, обеспечение доступности информации

авторизированным пользователям и сохранение целостности обрабатываемой информации.

Стратегической целью обеспечения информационной безопасности является содействие и укрепление процесса развития системы обеспечения информационной безопасности [3].

Обеспечение информационной безопасности должно осуществляться с учетом установленных, общих принципов, поскольку информационная безопасность является связующим элементом реализации информационной и национальной политики. К основным задачам в области обеспечения информационной безопасности на уровне государственного регулирования можно отнести следующие направления деятельности:

- 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 эффективности средств обеспечения информационной безопасности Российской Федерации;
- унификация информационных систем.

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.

Проанализировав задачи обеспечения информационной безопасности со стороны государства в целом и со стороны частных предприятий, следует перейти к более узкому исследованию направлений целей и задач на примере Федеральной налоговой службы Российской Федерации. 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 и предотвращение возможных нарушений в порядке и процессе доступа к информации, можно также выделить основные задачи обеспечения информационной безопасности ФНС России. К ряду последних следует отнести следующее:

- анализ реализации возможных угроз и ущерба, создание условий для предотвращения последствий нарушения в системе информационной безопасности;
- своевременная модернизация нормативно-правовой базы, регламентирующей деятельность Федеральной налоговой службы в области защиты информации;
- предотвращение возможности несанкционированного доступа в функционирование информационной системы Федеральной налоговой службы;
- своевременное внедрение соответствующих средств и мер защиты данных информационной системы;
- обеспечение полноценной отчетности и контроля выполнения всех действий, связанных с информационной системой Федеральной налоговой службы;
- обработка, хранение и использование достоверной и полноценной информации.

Главной целью обеспечения безопасности информации в ФНС России является предотвращение (минимизация) ущерба субъектам правоотношений

в результате противоправных действий с информацией, приводящих к ее разглашению, утрате, утечке, искажению (модификации), уничтожению или незаконному использованию, либо нарушению работы ИС налоговых органов и телекоммуникационной инфраструктуры ФНС России, используемой для информационного обмена и взаимодействия с органами государственной власти и организациями.

Основными целями обеспечения безопасности информации являются:

- предотвращение несанкционированного доступа к информации;
- предотвращение нарушений прав субъектов при обработке информации;
- предупреждение последствий нарушения порядка доступа к информации;
- недопущение воздействия на технические средства обработки информации;
- недопущение деструктивного информационного воздействия на информацию.

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

- совершенствование политики ФНС России в области ИБ при создании и внедрении ИС налоговых органов и телекоммуникационной инфраструктуры ФНС России;
- обеспечение соответствия мер и средств защиты информации в ИС налоговых органов положениям нормативных документов по безопасности информации;
- совершенствование нормативно-правовой базы обеспечения ИБ, координация деятельности налоговых органов по защите информации;
- обеспечение полноты, достоверности и оперативности получения информации налогоплательщиками и органами государственной

власти, а также информационной поддержки принятия управленческих решений центральным аппаратом ФНС России;

- защита от вмешательства в процесс функционирования ИС налоговых органов посторонних лиц, совершенствование СиЗИ, ее организации, форм и методов предотвращения и нейтрализации угроз ИБ, ликвидации последствий;
- предотвращение, в том числе с использованием организационно-правовых мер и технических средств защиты информации, несанкционированных действий и незаконных посягательств на ИР ФНС России со стороны посторонних лиц и работников ФНС России, не имеющих соответствующих полномочий;
- регистрация событий, влияющих на безопасность информации, обеспечение полной подконтрольности и подотчетности выполнения всех операций, совершаемых в ИС налоговых органов;
- своевременное выявление, оценка и прогнозирование источников угроз, причин и условий, способствующих нанесению ущерба интересам субъектов, нарушению нормального функционирования и развития ИС налоговых органов и телекоммуникационной инфраструктуры ФНС России
- анализ рисков реализации угроз, оценка возможного ущерба, предотвращение неприемлемых для ФНС России последствий нарушения ИБ, создание условий для минимизации, локализации и максимально возможного возмещения ущерба;
- обеспечение возможности восстановления актуального состояния ИС налоговых органов и телекоммуникационной инфраструктуры ФНС России при нарушении ИБ;
- создание системы управления информационной безопасностью.

Грамотное и конкретное определение актуальных задач на предприятии может помочь не только сократить материальный и моральный ущерб компании в случае реализации информационной угрозы, но и предотвратить возможные нарушения. Как правило, задачи обеспечения информационной безопасности сводятся к установлению определенных нормативов и стандартов в области безопасности, которые помогают обеспечить высокий уровень защищенности информации от несанкционированных или противоправных действий со стороны сторонних лиц или сотрудников предприятия.

Комплексное выполнение установленных стандартов безопасности оказывает влияние на эффективное функционирование системы обеспечения информационной безопасности. Таким образом, формирования основного перечня задач по защите информации предприятия определяет дальнейшее направление деятельности предприятия в области информации.

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 (IoT) 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. 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» [1]. Стратегия национальной безопасности дает нам 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 [13]. 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 [14]. Угроза информационной безопасности – это совокупность факторов и последствий, которые могут создать потенциальную или фактическую опасность состоянию защищенности личности, общества и государства. Такими факторами может быть весь перечень основных принципов функционирования Интернета. Среди них: принципы иерархичности, демократичности, децентрализации, конвергенции и экстерриториальности [15]. 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:

- 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. В первую очередь, необходимо определить, кто или что может представлять из себя источник угрозы информационной безопасности. Мной уже было отмечено ранее, что источником угрозы 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.

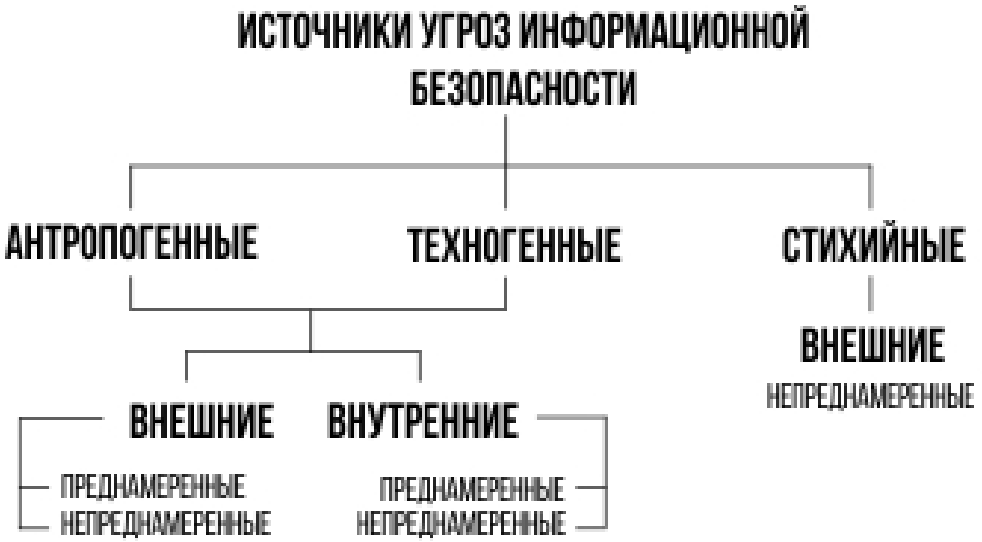


Рисунок 2 – Классификация по источнику угроз информационной безопасности[2]

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

[2] Составлено автором по: [33]

представляет основной, технический и вспомогательный персонал. К ним могут также относится и высококвалифицированные специалисты, работающих в сфере эксплуатации технических средств и программного обеспечения.

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 [38]. 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. Сам процесс осуществления угрозы, как правило состоит из четырех этапов: сбор информации, проникновение в среду, реализация несанкционированного доступа и ликвидация следов доступа. Классификация по способу реализации угрозы информационной безопасности состоит из следующих видов:

- 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:

1. Способ осуществления угрозы. Выделяют преднамеренные, случайные действия, а также чрезвычайные ситуации техногенного или природного характера.
2. Нацеленность угрозы на важнейшие свойства информации такие как: конфиденциальность, целостность, доступность. Именно против этих составляющих в первую очередь направлены информационные атаки.
3. Компоненты информационных технологий и систем. На что непосредственно нацелены угрозы: сети, данные, программно-аппаратные комплексы, иная поддерживающая инфраструктура, а также аппаратная часть информационной системы.
4. Локализация источника угрозы. Она может быть, как внутри информационной системы, так и вне системы или технологии.

Была рассмотрена основная и наиболее распространенная классификация угроз информационной безопасности. На данном этапе следует обратить внимание на более узкую классификацию, а именно на угрозы информационной безопасности систем уделенной обработки данных. 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:

- угрозы, которые связаны непосредственно с аппаратной частью информационной системы;
- угрозы, которые связаны с коммуникационной системой;

– угрозы, характерные для ПО.

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

Рисунок 3 – Классификация угроз информационной безопасности в информационных системах[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 [19]. 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.

[3] Составлено автором по: [27]

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 [27].

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:

1. 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.
2. Распределенная атака на отказ. В отличие от простой атаки на отказ, распределенная атака задействует большое количество рабочих станций.
3. Подделка пакетов управляющих сетевых устройств.
4. Перехват сетевого трафика.
5. Сканирование. Получение доступа к сетевым портам информационной системы с целью выявлении уязвимостей программного обеспечения.

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

1. Неправильная конфигурация аппаратных средств. Некорректная настройка аппаратной части может стать причиной физического повреждения или отказа работы аппаратуры.
2. Получение физического доступа к носителю информации.

3. 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 [20].
4. 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.

Классификация и идентификация угроз информационной безопасности предприятия являются одними из важнейших процессов для эффективной и безопасной работы.

1.3 Результаты и выводы первой главы

Были исследованы теоретические аспекты угроз информационной безопасности, рассмотрены основные задачи обеспечения информационной безопасности предприятия, а также была проведена подробная классификация угроз информационной безопасности.

Были изучены основные источники угроз информационной безопасности, которые могут оказать негативное воздействие на работу территориальных налоговых органов. Данная часть исследования имеет принципиальную значимость, поскольку своевременная идентификация и классификация угроз информационной безопасности необходима для эффективного обеспечения защиты информационных ресурсов.

В процессе исследования теоретической части были использованы работы отечественных и зарубежных авторов, электронные ресурсы, а также материалы, полученные в ходе участия в конференции «БИТ Безопасность информационных технологий – Урал 2020».

Были рассмотрены основные цели и задачи обеспечения информационной безопасности. Задачи сводятся к установлению определенных нормативов и стандартов в области безопасности, которые помогают обеспечить высокий уровень защищенности информации от несанкционированных или противоправных действий со стороны сторонних лиц или сотрудников предприятия.

2 АНАЛИЗ СУЩЕСТВУЮЩИХ МЕТОДИК 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 [21]. 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 [22]. 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.

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 [4].

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 [3]. 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.

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 количества новых технологий. Так, по данным специалистов компании «InfoWatch» к концу 2019 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% [23].

Основываясь на ведомственных статистических данных о состоянии судимости на 2019 год судебного департамента при Верховном Суде Российской Федерации, количество осужденных по ст.137 УК РФ составляет 171 человек, в 2018 году – 127, в 2017 году число осужденных составляло 86 человек [24]. Динамику роста преступлений, связанных с нарушением неприкосновенности частной жизни можно рассмотреть более наглядно на рисунке 4.

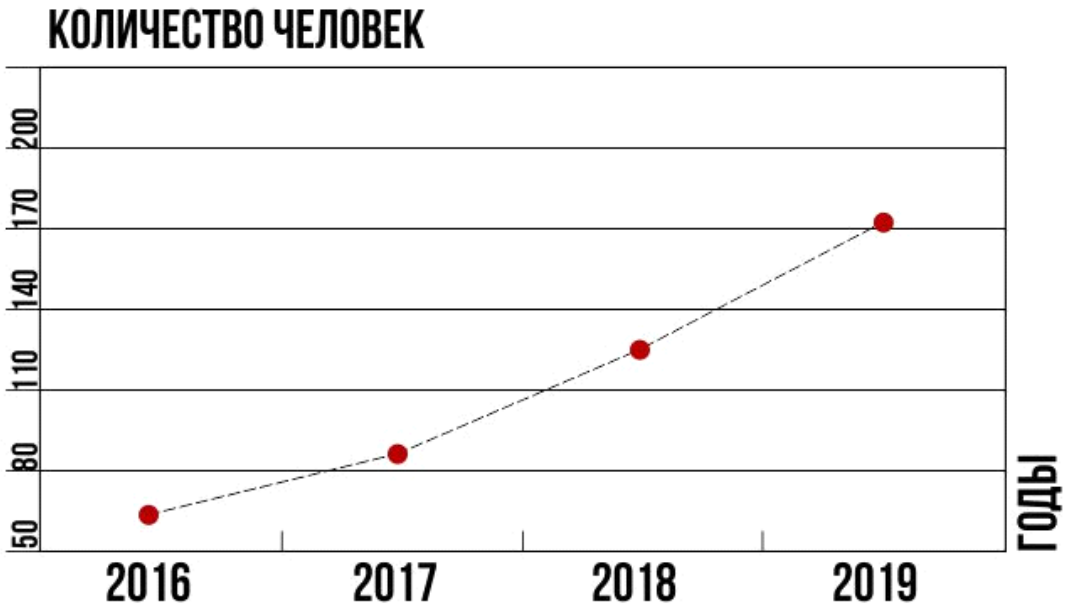


Рисунок 4 – Динамика числа осужденных по ст.137 УК РФ[4]

В представленном графике я использовала ст.137 УК РФ «О нарушении неприкосновенности частной жизни» для примера динамики уголовных преступлений, связанных с нарушением информационной безопасности. Осуждение по этой статье предполагает незаконное распространение или собирание информации [25]. Показатели количества осужденных по другим

[4] Составлено автором по: [24]

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 [26].

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.

За реализацию положений Концепции отвечают лица, входящие в организационную структуру системы обеспечения безопасности информации ФНС России, в том числе:

- структурные подразделения центрального аппарата ФНС России;
- территориальные органы и подведомственные учреждения ФНС России;
- научно-исследовательские организации ФНС России;

– разработчики ИС и объектов информатизации ФНС России.

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 Федеральной налоговой службе 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.

1. 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 [27]. 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. 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[5]

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

2. 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

[5] Составлено автором по: [27]

будет зафиксирована в системе Федерального информационного ресурса, после чего последует процесс идентификации данного нарушения.

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.

3. 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.

Все возможные угрозы безопасности информации идентифицируются следующим образом:

$УБИ_j$= [источник угрозы; уязвимости; способы реализации; объекты воздействия; последствия]

Выявленная таким образом угроза информационной безопасности подлежит нейтрализации.

5. 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. Оценка вероятности реализации угроз осуществляется следующим образом:

$$\text{УБИ}_j^A = [\text{вероятность реализации угрозы } (P_j);\ \text{степень ущерба } (X_j)]$$

6. 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 [54]:

- 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.

7. 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.

Страхование средств обработки информации направлено на компенсацию ущерба ФНС России в случае утраты информационных ресурсов. Страхование средств обработки информации включает страхование ответственности организаций и производителей информационной системы, обеспечивающих функционирование информационной системы ФНС России.

Введение системы надбавок и коэффициентов подразумевает создание определенных льготных выплат сотрудникам ФНС России, деятельность которых связана с конфиденциальной информацией. Система формируется исходя из стажа работы сотрудника в ФНС России [56].

Были 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 [58]. Kaspersky Security является одним из самых современных антивирусных программ, обеспечивающий базовую защиту ПК. 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 ПК;
- задействование процесса мониторинга ссылок перед переходом на сайт;
- высокий уровень защиты ПК 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 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 [59].

Для объектов информатизации ФНС актуальными и основными источниками внешних антропогенных угроз безопасности информации являются [48]:

- 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.

К основным техногенным источникам угроз можно отнести неблагоприятные события техногенного характера, включая аварии на средствах телекоммуникационной инфраструктуры, на средствах инженерных коммуникаций, отказы и сбои в работе оборудования.

Для объектов ФНС актуальными уязвимостями являются [48]:

- 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, к которым можно отнести: недовольство положением, недовольство действиями руководства, психологическая несовместимость некоторых сотрудников, психосоматическое и физическое состояние;
- восприимчивость программного обеспечения к вирусам и вредоносным программам;
- возможность несанкционированной модификации программных вызовов, кода, использование среды программирования автоматизированной информационной системы;
- уязвимости СиЗи (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, актуальность, 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, с 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 2 представлены угрозы с наивысшим уровнем актуальности и высоким уровнем возможной реализации.

Таблица 2 – Перечень угроз с наивысшим уровнем возможной реализации[6]

Наименование угрозы безопасности информации	**Опасность**	**Вероятность реализации**	**Y1**	**Возможность реализации**	**Актуальность**
Угроза обнаружения открытых портов и идентификации привязанных к нему сетевых служб	Средняя	Высокая	1	Очень высокая	Актуальная
Угроза маскирования действий вредоносного кода	Высокая	Средняя	0,75	Высокая	Актуальная
Угроза обнаружения хостов	Средняя	Высокая	1	Очень высокая	Актуальная

[6] Составлено автором по: [27]

Окончание таблицы 2 – Перечень угроз с наивысшим уровнем возможной реализации

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

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.

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.

2.2 Результаты и выводы второй главы

Анализ существующей нормативно-правовой базы привел к выводу, что отечественная правовая система в области защищенности информации имеет большое количество изъянов.

Были проанализированы основные методы выявления и противодействия угроз информационной безопасности на предприятии. К основным методам выявления относятся: экспертный метод, системный метод, метод идентификации возможных угроз и метод оценки вероятности реализации угроз. К основным методам противодействия угроз информационной безопасности на предприятии можно отнести правовые и экономические методы. Проанализированные методы выявления и противодействия угроз являются актуальными и основными в процессе обеспечения информационной безопасности ФНС России. Рассмотренные методы имеют ряд достоинств и недостатков, и нуждаются в дальнейшем усовершенствовании для более эффективного обеспечения информационной безопасности предприятия.

Был выявлен список наиболее вероятных и актуальных угроз для безопасности информации Федеральной налоговой службы. Количество возможных угроз очень разобщено, что приводит к усложнению своевременного процесса выявления. Обширный спектр возможных угроз и усложненный процесс выявления может повлечь за собой существенный ущерб предприятия.

В ходе анализа действующей методики определения уровня защищенности и актуальности угроз были выявлены определенные сложности. Ключевые недостатки данный методики касаются неопределенного значения показателей.

Значительным недостатком также является и тот факт, что 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 РАЗРАБОТКА МЕТОДИКИ ПРЕДОТВРАЩЕНИЯ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ С ЦЕЛЬЮ МИНИМИЗАЦИИ УЩЕРБА

3.1 Общая характеристика предприятия и построения полной модели

Федеральная налоговая служба является федеральным органом исполнительной власти, который осуществляет функции по контролю и надзору за соблюдением законодательства о налогах и сборах, за правильностью исчисления, за своевременностью и полнотой внесения в соответствующий бюджет налогов и сборов, в случаях, предусмотренных законодательством Российской Федерации, за правильностью исчисления, полнотой и своевременностью внесения в соответствующий бюджет иных обязательных платежей [8]. Действующая Федеральная налоговая служба была основана 19 марта 2004 года, объединившая в себе Государственную налоговую службу, Министерство Российской Федерации по налогам и сборам и Федеральную службу по банкротству и финансовому оздоровлению.

По последним данным, опубликованным Министерством Финансов, количество сотрудников Федеральной налоговой службы, составляет 146 000 человек, что составляет 23% от общего числа федеральных сотрудников [28]. Существует 85 территориальных объектов Управления Федеральной налоговой службы России по субъектам РФ и 9 межрегиональных инспекций по Федеральным округам, которые в свою очередь, подразделяются на инспекции по крупнейшим налогоплательщикам, инспекции по городам и инспекции по районам [29].

Количество пользователей информационных ресурсов ИТ-инфраструктуры ФНС России составляет 120 000 человек, в том числе 10 000 - федерального уровня, 30 000 – регионального уровня и 80 000 местного уровня [29].

Основные направления деятельности Федеральной налоговой службы России регламентированы стратегической картой ФНС России и могут меняться с истечением срока действия. Основные направления деятельности ФНС на 2020-2024 годы [29]:

- обеспечение соблюдения действующего законодательства о сборах и налогах;
- создание соответствующих условий для исполнения налоговых обязанностей налогоплательщиками;
- упрощение процедур и снижение административной нагрузки, развитие коммуникации с обществом и бизнесом;
- оптимизация деятельности налоговых органов в соответствии с затратами на ее осуществление;
- совершенствование и укрепление кадрового потенциала.

В соответствии с основными направлениями деятельности ФНС осуществляет следующие полномочия:

- ведение полного учета денежных средств у индивидуальных предпринимателей и в организациях;
- осуществление валютных операций резидентами и нерезидентами, которые не являются кредитными организациями;
- полное и своевременное внесение в соответствующий бюджет обязательных платежей;
- полное и своевременное внесение налогов и сборов.

Основной миссией Федеральной налоговой службы является эффективная деятельность по осуществлению контроля и надзора, а также предоставление качественных услуг для комфортного, законного и прозрачного ведения бизнеса, формирования финансовой основы деятельности государства и соблюдения конституционных прав налогоплательщиков [46]. Основными направлениями для формирования

стратегических целей налоговых органов, в соответствии со стратегической картой ФНС России, на 2020-2024 год являются: ожидания Правительства РФ, общества и бизнеса, и повышение внутренней эффективности. Данные основные направления формируют список стратегических целей, который полностью совпадает с основными направлениями деятельности ФНС, рассмотренными ранее. Каждая из стратегических целей предполагает решение ряда задач, к данным задачам относятся:

- обеспечение законности, мотивированности и обоснованности решений, принимаемых сотрудниками ФНС;
- совершенствование функциональной и организационной модели ФНС;
- внедрение актуальных ИТ-технологий и развитие централизации в процессе обработки данных;
- повышение уровня коммуникативных и профессиональных навыков сотрудников ФНС;
- распространение опыта налогового администрирования;
- развитие принципа информационной открытости;
- совершенствование системы надзора и контроля за соблюдением валютного законодательства РФ;
- совершенствование процедуры регистрации;
- развитие удаленного доступа и электронного взаимодействия, повышение эксплуатации телекоммуникационных каналов связи;
- диверсификация сервисных услуг и повышение уровня качества обслуживания;
- проведение регулярной профилактики нарушений посредством развития внутреннего аудита и контроля.

Основными показателями эффективности, по которым можно оценить достигаются ли поставленные цели Федеральной налоговой службы, являются [29]:

– увеличение процента собираемости налогов и сборов;
– повышение степени разработки единого реестра субъектов;
– увеличение процента удовлетворённости граждан качеством услуг;
– снижение человеко-часов, затраченное в процессе реализации дополнительных программ;
– соотношение объема поступлений по налогам и сборам к объему задолженности по налогам и сборам.

Федеральная налоговая служба предоставляет большой спектр услуг. Классификация услуг представлена на рисунке 5.

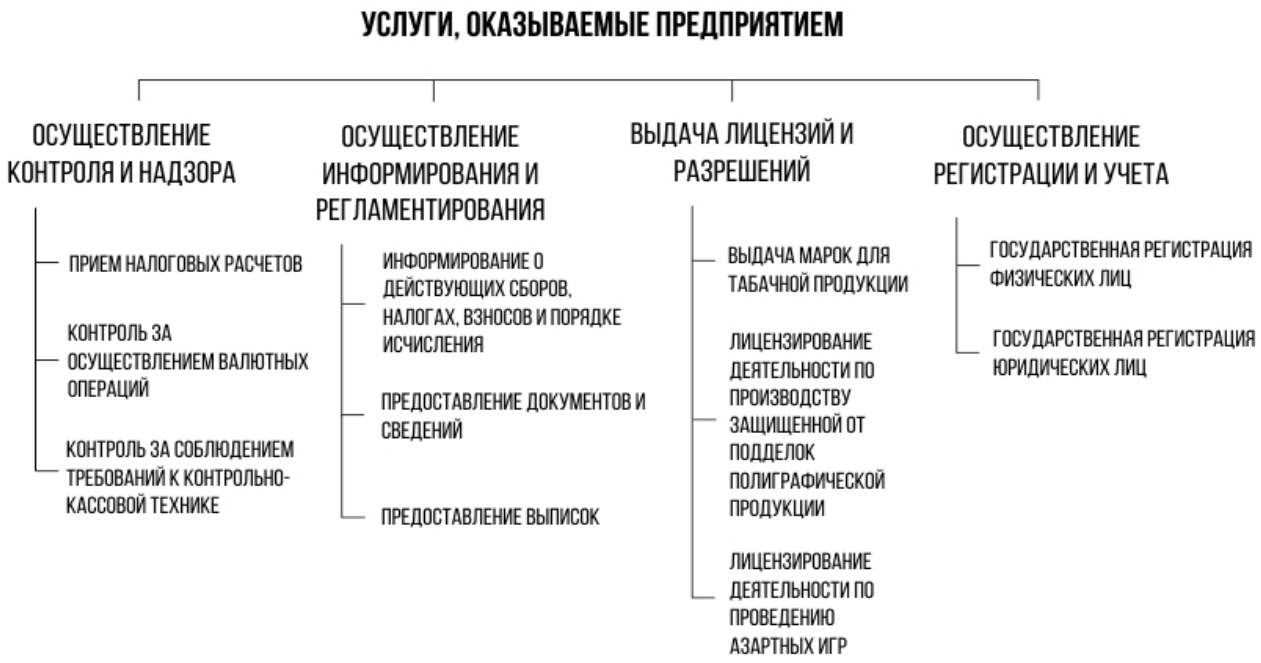


Рисунок 5 – Услуги предприятия[7]

Федеральная налоговая служба предоставляет следующий перечень электронных и неэлектронных государственных услуг населению:

– информирование граждан о действующих сборах, налогов, взносов, порядке исчисления и уплаты налогов, правах и обязанностях, законодательстве о налогах и сборах;

[7] Составлено автором по: [29]

- предоставление документов и сведений, содержащихся в Едином государственном реестре;
- предоставление выписки из Единого государственного реестра;
- государственная регистрация физических и юридических лиц;
- сведения о доходах физического лица по форме 2-НДФЛ
- прием налоговых расчетов;
- выдача марок для табачной продукции, произведенной на территории РФ;
- контроль за осуществлением валютных операций нерезидентами и резидентами;
- лицензирование деятельности по производству защищенной от подделок полиграфической продукции;
- лицензирование деятельности по проведению азартных игр в тотализаторах и букмекерских конторах;
- контроль за соблюдением требований к контрольно-кассовой технике.

Миссия о основные стратегические цели представлены на рисунке 6.

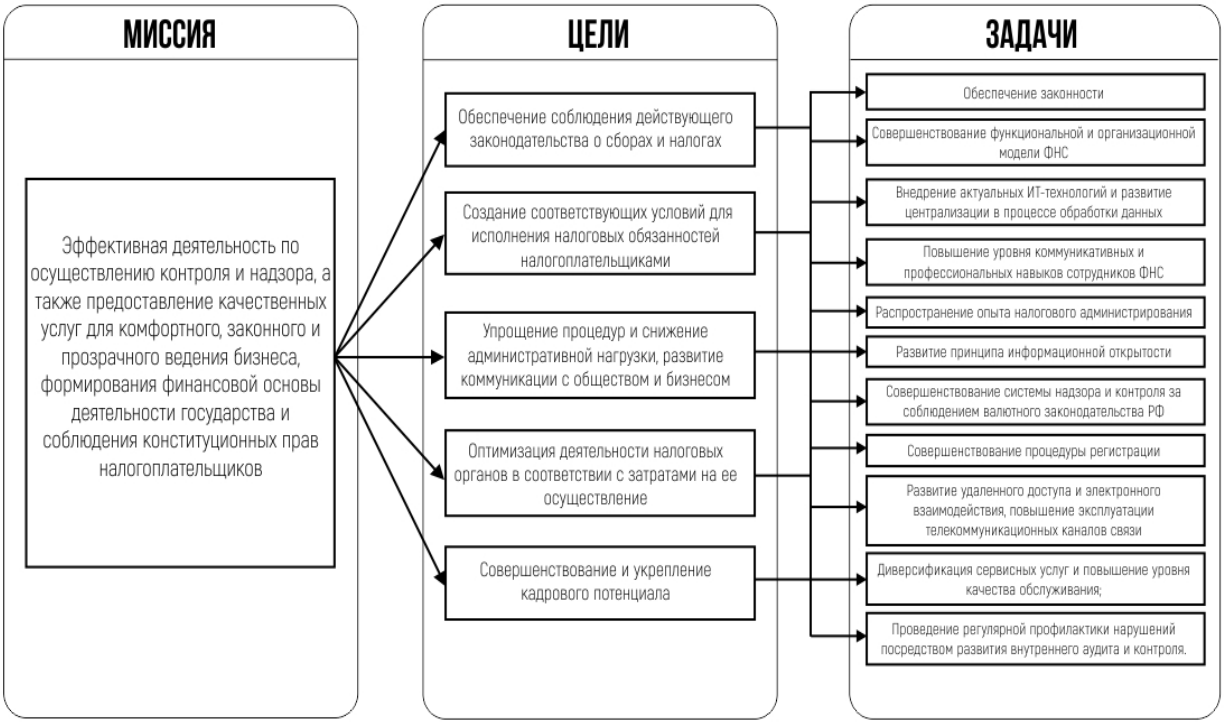


Рисунок 6 – Стратегические цели и задачи ФНС[8]

Для наглядного представления полной модели предприятия, определение основных факторов успеха, ключевых показателей эффективности и стратегий представлен рисунок 7.

[8] Составлено автором по: [8,29]

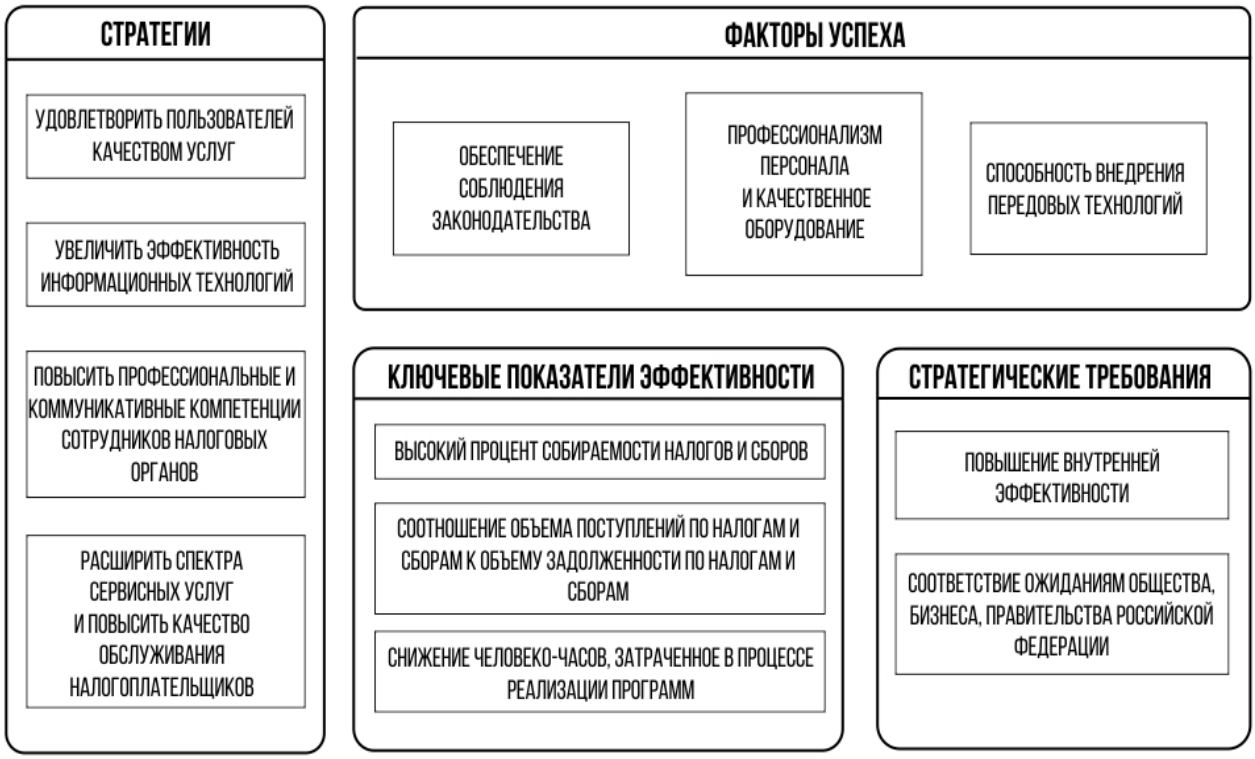


Рисунок 7 – Основные факторы успеха, стратегии и ключевые показатели эффективности предприятия[9]

Процессы, осуществляемые ФНС России, можно определить в совокупность следующих основных направлений. Каждое из этих направлений отвечает за выполнение определенной бизнес-функции. Бизнес-процессы представлены на рисунке 8.

[9] Составлено автором по: [8,29,55]

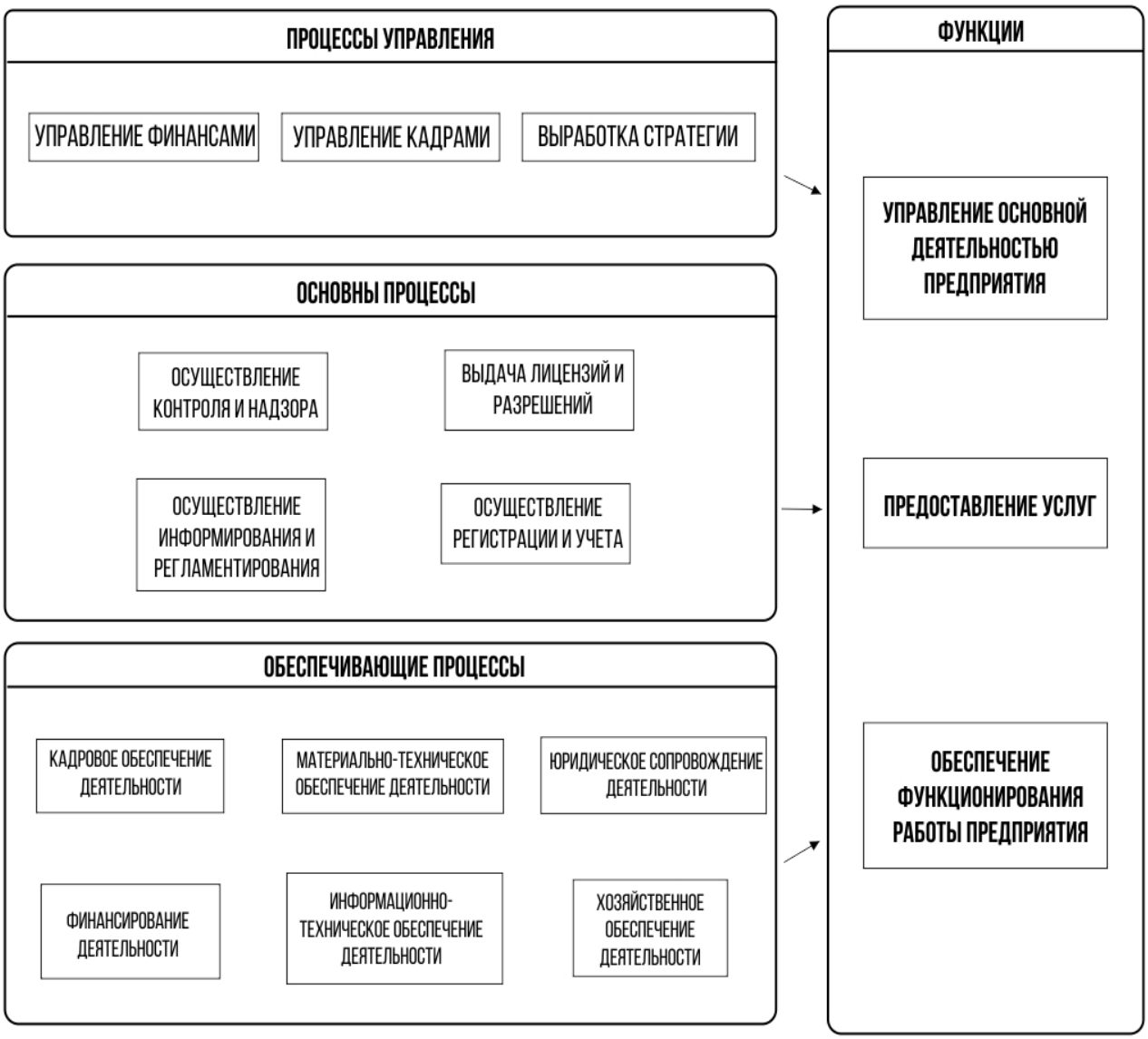


Рисунок 8 – Бизнес-процессы[10]

Единую централизованную систему налоговых органов составляют управления службы по субъектам Российской Федерации, межрегиональные инспекции, инспекции по районам, районам в городах и в городах без районного деления. Организационную структура ФНС России представлена на рисунке 9.

[10] Составлено автором по: [8,29,55]

Рисунок 9 – Организационная структура ФНС России[11]

Актуальная организационная структура центрального аппарата управления ФНС России на 2020 год представлена на рисунке 10.

[11] Составлено автором по: [49]

Рисунок 10 – Схема структуры централизованного аппарата ФНС России[12]

[12] [29]

Все стадии развития государства требуют от системы налоговых органов обеспечения своевременного сокращения внутреннего и внешнего долга, обработку и поступление налоговых платежей на всех уровнях государственной и муниципальной власти, а также координирование бюджета по расходам и доходам [55]. Наиболее приоритетной задачей в процессе функционирования налоговой системы является своевременное обеспечение налоговых поступлений. На данном этапе современное устройство государства предполагает в том числе и эффективную автоматизацию деятельности налоговых органов, поскольку прогрессивное развитие цифровых и информационных технологий формирует принципиально иной уровень управления во всех областях жизнедеятельности общества.

Федеральная налоговая служба России располагает большим количеством программных средств для налогоплательщиков. Модель информационной системы представлена на рисунке 11.

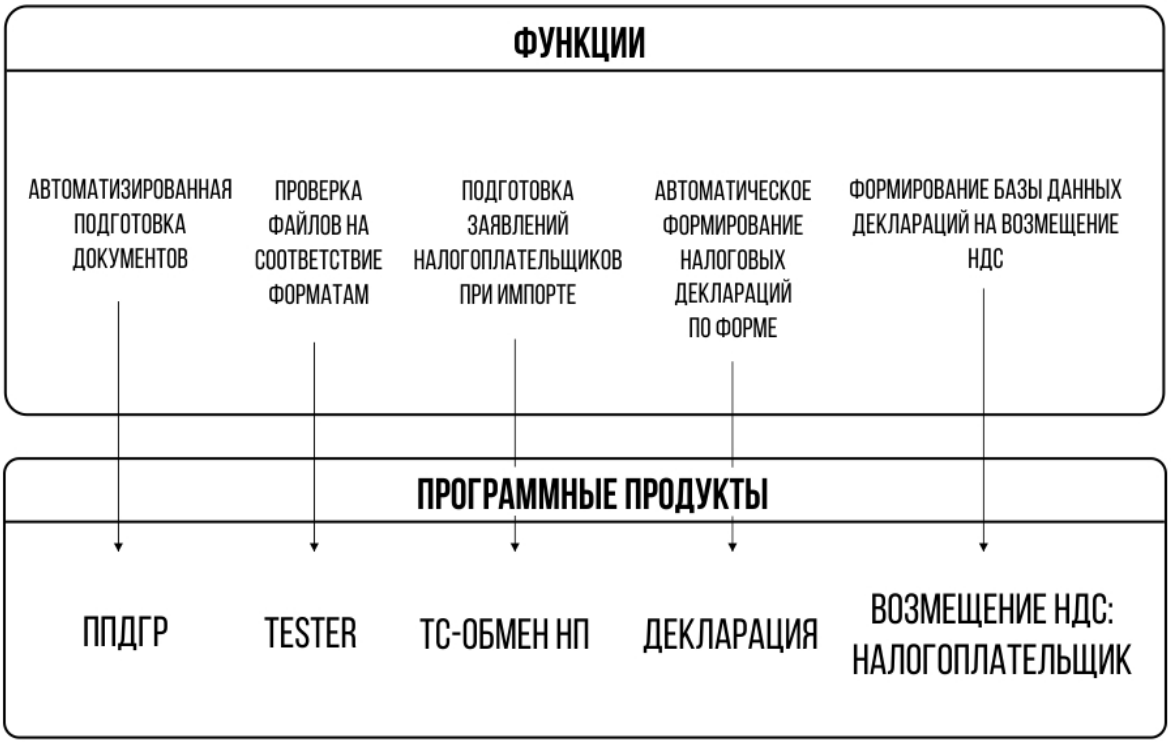


Рисунок 11 – Связь функций и программных продуктов ФНС[13]

[13] Составлено автором по: [29,58]

Рассмотрим более подробно процессы разработки, внедрения и модернизации информационных технологий в сфере системы налогообложения. Прежде всего, необходимо определить область деятельности ФНС, она включает в себя: контроль за соблюдением законодательства в области налогообложения, корректное исчисление, регулярное и своевременное внесение денежных средств в соответствующий бюджет и осуществление регламентированных функций налогового органа. Необходимо отметить, что ФНС РФ является уполномоченным федеральным органом исполнительной власти, в перечень функций которого также относятся такие виды деятельности, как регистрация физических и юридических лиц, и обеспечение процедуры банкротства.

Одной из основных задач Федеральной налоговой службы Российской Федерации является корректное и рациональное использование информационных технологий в процессе своей работы, а также применение автоматизированных систем и баз данных для достижения более высокого уровня эффективности [50]. Автоматизированная система управления ФНС России представлена на рисунке 12.

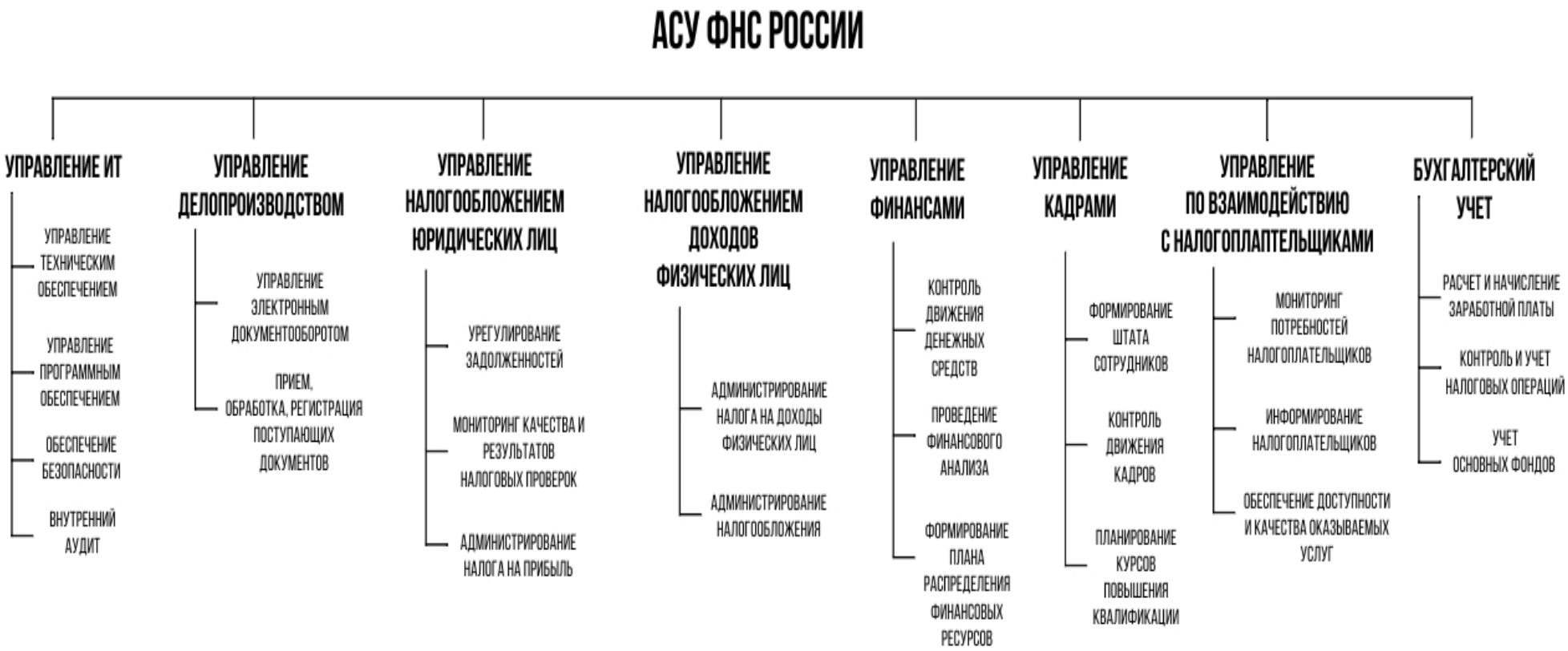


Рисунок 12 – Функциональная схема АСУ ФНС России[14]

[14] Составлено автором по: [58]

Реализацию своих функций ФНС России осуществляет на основе использования прикладного программного обеспечения автоматизированной информационной системы «Налог-3», автоматизированной информационной системы «Маркировка» и Федеральной информационной адресной системой [57].

ИТ-инфраструктура ФНС России представляет собой единую информационную систему ФНС России, обеспечивающую автоматизацию деятельности ФНС России по всем выполняемым функциям, определяемым Положением о Федеральной налоговой службе, в том числе приём, обработку, предоставление данных и анализ информации, формирование информационных ресурсов налоговых органов, статистических данных, сведений, необходимых для обеспечения поддержки принятия управленческих решений в сфере полномочий ФНС России и предоставления информации внешним потребителям.

ИТ-инфраструктура ФНС России включает в себя следующие зарегистрированные в установленном порядке системы АИС «Налог-3», в том числе автоматизированные системы контроля ККТ, НДС 2, ГИР БО, Интернет-сервисы ФНС России, ЕГРЮЛ, ЕГРИП), АИС «Маркировка» (Аналитический сегмент) и ФИАС (ГАР). Целевая архитектура АИС «Налог-3» представлена на рисунке 13 [51].

Рисунок 13 – Целевая архитектура АИС «Налог-3»[15]

ИТ-инфраструктура ФНС России создана с целью повышения эффективности реализации полномочий и решения задач, определённых в Положении о ФНС России.

ИТ-инфраструктура ФНС России направлена на решение следующих задач:

- обеспечение "открытости" налоговых органов для налогоплательщика, путём упрощения процедур его взаимодействия с ФНС России и перевода их в электронный вид;
- создание единого информационного массива и подключение налоговых органов к новым внешним источникам информации;
- гарантированное соблюдение регламентных процедур налогового администрирования, качество и сроки их реализации;

[15] [57]

- снижение текущих издержек налогового администрирования, в первую очередь за счёт создания и внедрения электронной системы массовой обработки сведений, поступающих в налоговые органы;
- совершенствование процедур информационного взаимодействия с органами государственной власти и местного самоуправления;
- обеспечение контроля над налоговой деятельностью налогоплательщика путём создания единого и достоверного ресурса, содержащего всю информацию по конкретному налогоплательщику ("досье" налогоплательщика), в том числе сведения, позволяющие своевременно выявлять признаки ухода от уплаты налогов;
- обеспечение автоматизированного мониторинга деятельности Федеральной налоговой службы со стороны руководства налоговых органов;
- повышение качества контрольной работы, в том числе за счёт комплексного использования, созданного единого информационного ресурса и подключения налоговых органов к новым внешним источникам информации;
- повышение качества принятия решений, анализа и прогнозирования за счёт создания аналитических инструментов, позволяющих проводить анализ и прогнозирование налоговых поступлений с учётом макроэкономических показателей и внешних факторов.

ИТ-инфраструктура ФНС России функционирует в рамках телекоммуникационной инфраструктуры, построенной в соответствии с Единым Проектным решением по телекоммуникационной инфраструктуре налоговых органов. ИТ-инфраструктура предприятия, обеспечивающая процессы управленческого персонала, является конфиденциальной

информацией, поэтому была рассмотрена ИТ-инфраструктура обеспечивающая взаимодействие с налогоплательщиками, она представлена на рисунке 14.

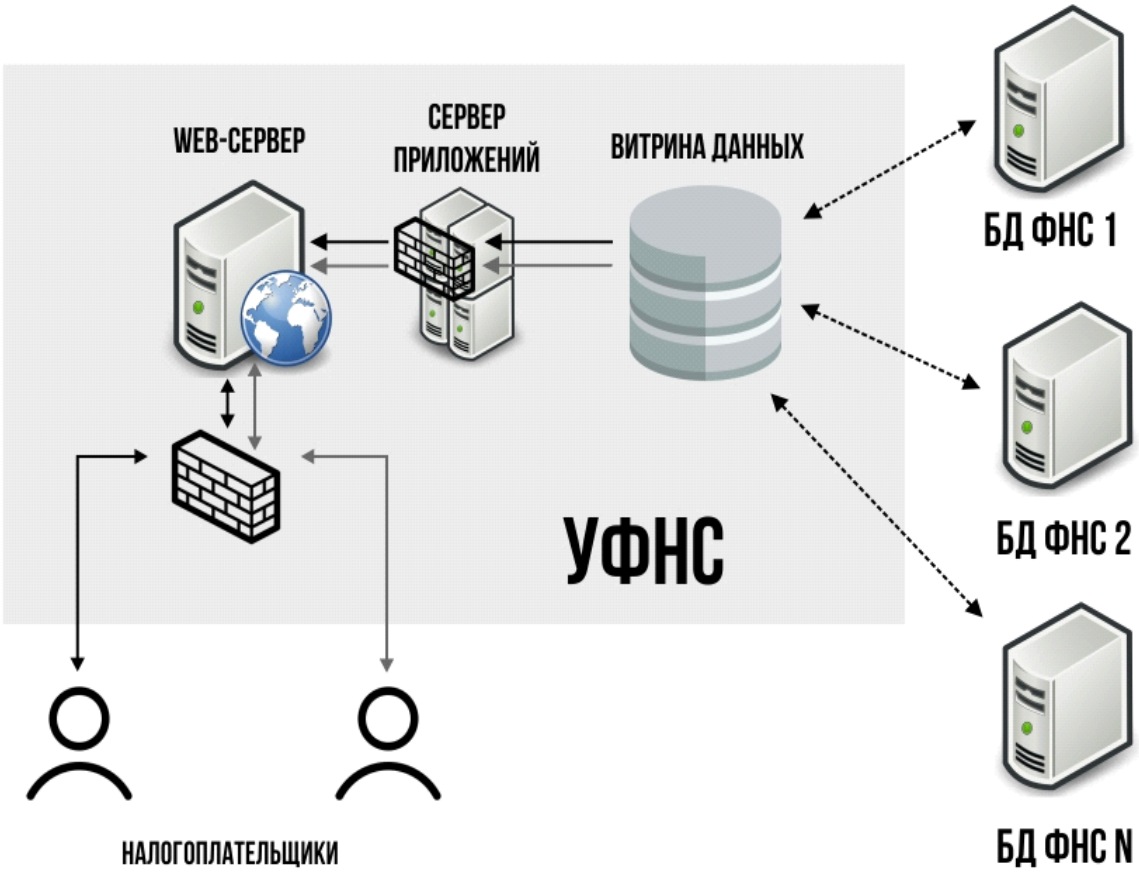


Рисунок 14 – ИТ-инфраструктура обеспечивающая информационное воздействие с налогоплательщиками[16]

Также, необходимо упомянуть и о транспортной инфраструктуре системы телекоммуникаций ФНС России. Данная инфраструктура организована на базе услуги IP MPLS VPN, обеспечивающей IP видимость между всеми объектами автоматизации в рамках сети Единого оператора связи, также имеющий распространенное название «Основной оператор связи ФНС России». Стоит отметить, что существует и аналогичная резервная сеть связи, построенная на основе спутниковых каналов передачи данных, предоставляемая «Резервным оператором связи ФНС России».

[16] Составлено автором по: [43]

На транспортную инфраструктуру сети операторов связи в системы телекоммуникаций ФНС России накладывается инфраструктура крипто-защищённых VPN-каналов. Трафик доступа в сети интернет передаётся в рамках сети IP MPLS VPN оператора связи в открытом виде. Трафик системы видеоконференцсвязи, охватывающей центральный аппарат ФНС России, межрегиональную инспекцию Федеральной налоговой службы по централизованной обработке данных ФНС России, и Управление Федеральной налоговой службы по субъектам Российской Федерации, находящимся в границах федерального округа, передаётся в защищённом виде через независимую инфраструктуру криптотуннелей [39].

Телекоммуникационные узлы объектов автоматизации состоят из следующих типов оборудования:

- крипто-маршрутизаторы;
- голосовые шлюзы и другое оборудование IP-телефонии;
- УАТС (офисная автоматическая телефонная станция);
- коммутирующее оборудование локальных вычислительных сетей;
- маршрутизаторы системы контроля и управления трафиком.

АИСН или автоматизированная информационная система налогообложения представляет одну из форм организационного управления налоговыми органами с применением новых информационных технологий и современных способов обработки данных [37]. С учетом задействования автоматизированной информационной системы налогообложения, в процессе функционирования которой применяются экономическо-математические методы, использована вычислительная техника и средства связи, повышается уровень рациональности и своевременности принимаемых решений, появляется возможность оптимальной организации информации и процессов администрирования, снижается трудоемкость обработки и сбора данных.

Можно выделить следующие основные цели автоматизированной информационной системы налогообложения:

- повышение уровня оперативности и производительности труда сотрудников ФНС;
- повышение уровня эффективности рабочего процесса ФНС благодаря оперативности принимаемых решений;
- обеспечение достоверной и своевременной информацией о правовых изменениях в налоговом законодательстве;
- уменьшение массива бумажного документооборота;
- обработка и анализ информационных данных для составления прогноза динамики поступления платежей в соответствующие бюджеты страны.

Корректная и исправная работа АИСН обеспечивает высокий уровень эффективности работы всех направлений деятельности налоговой системы.

Область деятельности налоговой службы изначально предполагала необходимость использования средств информатизации, которые связаны с хранением и обработкой большого количества информационных данных. Это стало причиной достаточно оперативного появления и внедрения специализированных программ на этапе развития налоговой службы современной России. Как правило, данные программы разрабатывались под конкретную задачу и распространялись по внутренней сети. Каждая инспекция владела разным перечнем программ, которые также имели свои отличающиеся особенности функционирования. 1998 год был ознаменован разработкой программ «Кольцо» и «ИС НИСТ», 2002 год – «АИС2-Налог» и «ЕГАИС» [37].

Стоит отметить, что изначальная архитектура актуальной АИС ФНС была разработана практически 15 лет назад. В 2006 году был принт проект по модернизации архитектуры информационной системы Федеральной налоговой службы России [57]. За первые три года реализации проекта

модернизации были разработаны и внедрены прикладные подсистемы АИС ФНС России, но в то же время использовались и введенные ранее программные информационные комплексы, что, в свою очередь, спровоцировало применение в процессе работы задействование старых и новых технологий управления баз данных в совокупности. Подобное устройство системы спровоцировало значительное усложнение и разобщенность в процессах автоматизации налогового администрирования, появлению трудностей в процессе сопровождения и технической поддержки, а также необходимость задействование IT-специалистов широкого профиля в системе налоговых органов [51].

С начала модернизации архитектуры информационной системы ФНС России произошел и ряд существенных изменений в области правового регулирования налоговых нормативов, особенно по отношению к использованию персональных данных, как сотрудников налоговых органов, так и налогоплательщиков. Процесс развития информатизации и цифровизации государственных услуг, в том числе системы налогообложения предполагает появления нового ряда нормативной базы, регулирующей сферу информационного взаимоотношения, в связи с которым необходимы соответствующие изменения основных направлений развития процессов налогового администрирования.

АИС «Налог» является автоматизированной информационной системой, направленной на повышение уровня эффективности за счет учетно-аналитической функции, упрощение работы налоговых органов и регулирование взаимоотношений налогоплательщиков и налоговых органов [58]. Использование данной информационной системы имеет ряд достоинств и недостатков. Например, к достоинствам рассматриваемой автоматизированной информационной системы является возможность предоставления налоговой декларации в режиме online или сокращение возможных ошибок при вводе данных. Также, процесс автоматизации налогового органа помогает в решении таких задач, как: автоматизация

подготовки, сбора, хранение и распределение различных информационных данных, создание необходимых для работы информационных ресурсов, автоматизация бизнес-процессов. Систематизированный перечень выявленных достоинств и недостатков можно рассмотреть более подробно на рисунке 15.

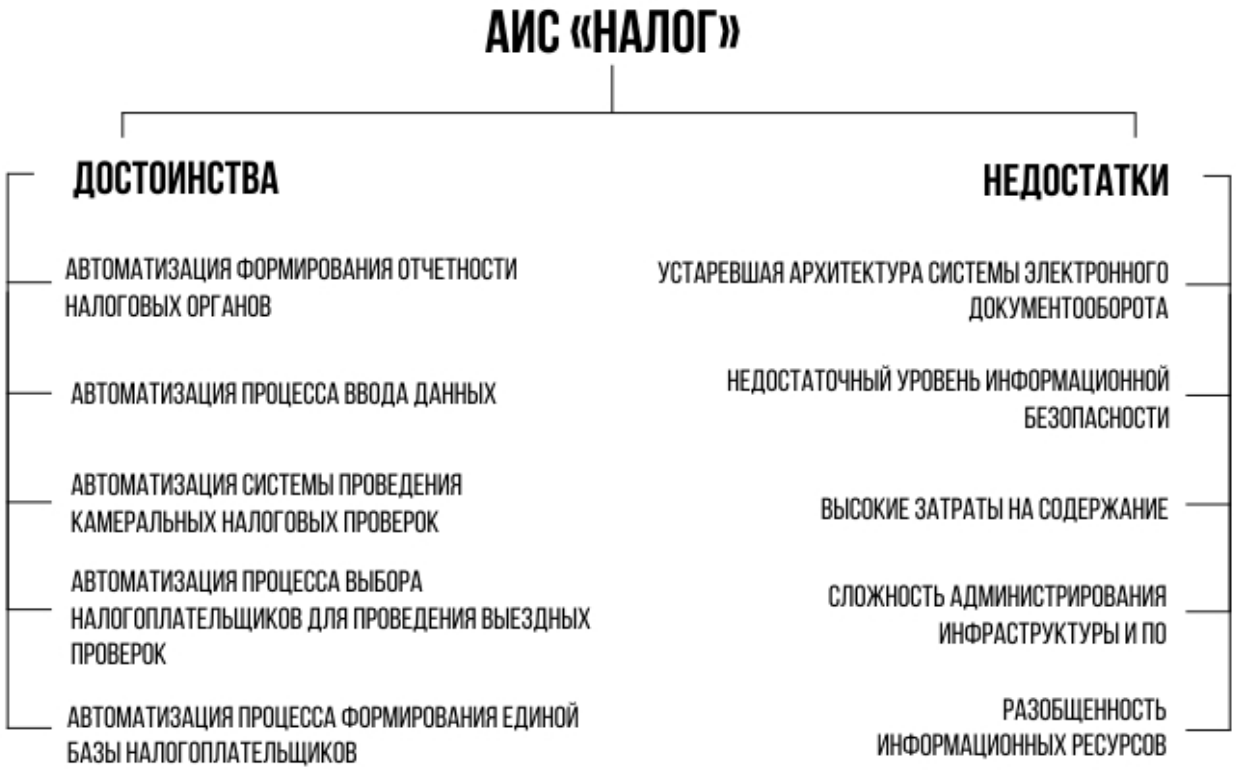


Рисунок 15 – Основные достоинства и недостатки АИС «Налог»[17]

Таким образом, была рассмотрена действующая автоматизированная информационная система Федеральной налоговой службы.

Полная модель предприятия изображена на рисунке 16.

[17] Составлено автором по: [51,57,58]

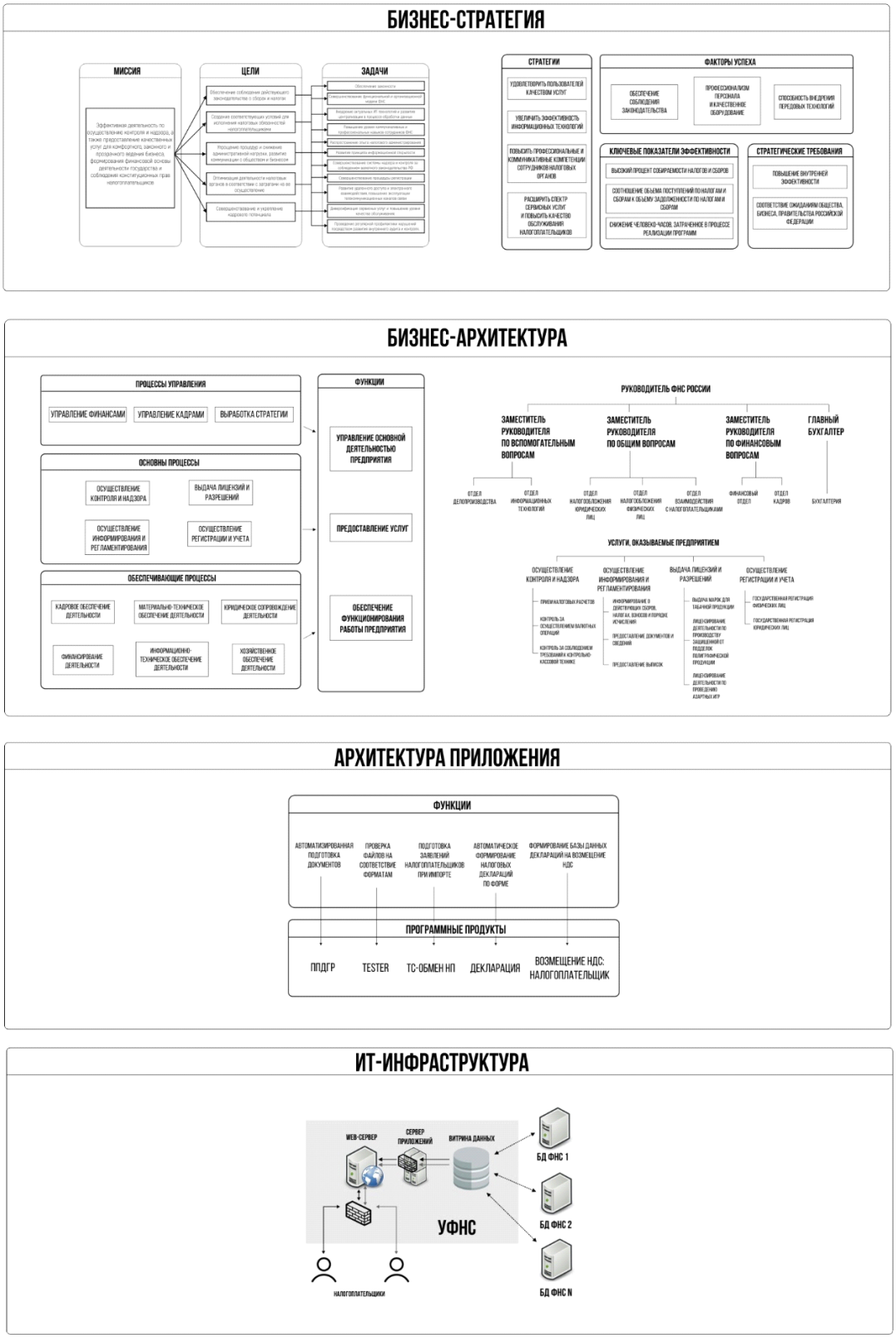


Рисунок 16 – Полная модель предприятия[18]

[18] Составлено автором по: [8,29,43,49,55,57,58]

3.2 Разработка комплексного плана мероприятий, направленного на сокращение угроз информационной безопасности

Комплексный план мероприятий, направленный на сокращение угроз информационной безопасности предполагает разработку нормативно-правовой базы, регулирующей деятельность отдела информационной безопасности по работе с угрозами, внедрение новых, более подходящих под специфику деятельности предприятия, программных продуктов в качестве инструментов контроля, мониторинга и устранение уязвимостей, а также разработку регламентов, методических рекомендаций и памяток, обеспечивающих сотрудников отдела достаточным количеством информации по работе с выявлением и устранением угроз, а также мероприятия, направленные на обучение специалистов: специалистов и начальников отдела, которые включают протокол оперативного совещания.

Организационно-распорядительная документация второго уровня в области обеспечения информационной безопасности играет важную роль в процессе обеспечения безопасности предприятия. К документации второго уровня относятся регламенты, инструкции и методические рекомендации, которые позволяют определить методы и порядок деятельности по защите от угроз информационной безопасности.

В соответствии с темой исследования, будут разработаны методические рекомендации, определяющие методы и порядок выявления угроз информационной безопасности. Методические рекомендации в данном контексте подразумевают определенный перечень унифицированных методов и правил выполнения функций по выявлению угроз информационной безопасности независимо от исполнителя. Формулы расчета показателей актуальности угроз информационной безопасности также указаны в методических рекомендациях [27]. Действующие методические рекомендации по выявлению угроз на предприятии были разработаны ФСТЭК России и проанализированы в предыдущей главе.

Действующая методика определения угроз исключает необходимость разработки новой методики, но, определив ее слабые положения, появляется необходимость в корректировке. В первую очередь, необходимо определить область применения данного документа. В действующей методике, она рассчитана исключительно на информационные системы персональных данных. Таким образом, в первую очередь, необходимой корректировкой данной методики определения угроз является область применения:

- методика определения угроз информационной безопасности должна использоваться для любых объектов, к которым утверждены требования по защите;
- создание возможности разработки ведомственных методик, учитывая специфику деятельности объекта.

Следующие требования в корректировке действующей методики можно отнести к процессу вычисления коэффициентов и определения значений:

- использование базы данных угроз при моделировании угроз информационной безопасности;
- установление конкретных определений при оценке незначительных и значимых негативных последствий;
- исключение неактуальных угроз из перечня расчета для более рационального распределения времени;
- отказ от неудобных в использовании параметров вероятности реализации угрозы и исходной защищенности информационной системы.

Следующие изменения необходимы в области проведения определенного ряда мероприятий, направленных на процесс определения угроз информационной безопасности.

- мероприятия, которые позволяют точно и корректно определить возможный источник угрозы. Использование информации о

возможных техниках и тактиках реализации той или иной угрозы, оценке рисков и проведение тестирования на проникновение;

- диверсификация вариантов осуществления мероприятий по определению актуальности угроз. Определение степени потенциальных последствий от способа реализации угрозы различными способами;
- обеспечение методики определения угроз конкретными примерами выполнения мероприятий, осуществляющих в целях определения актуальности той или иной угрозы информационной безопасности.

Данные изменения позволят обеспечить сотрудников отдела информационной безопасности ФНС России более структурированным и целостным планом по осуществлению мероприятий с целью определения угроз информационной безопасности.

В отличие от методических рекомендаций регламент определяет непосредственно порядок взаимодействия сотрудников и подразделений предприятия в рамках процесса выявления и устранения угроз информационной безопасности. Регламент информационной безопасности ориентирован на защиту информационных активов от угроз, представляющих, как правило, противоправные действия злоумышленников, а также на снижение потенциального ущерба в результате непреднамеренных действий персонала, технических аварий, нарушение процессов передачи, обработки и хранения информации, а также обеспечение должного функционирования всех процессов, направленных на защиту информации.

Отдел информационной безопасности ФНС России руководствуется следующими регламентами: регламент антивирусной защиты, парольной защиты, расследования инцидентов, предоставления доступа к информационным ресурсам и сервисам. Данный перечень регламентов не затрагивает область выявления и предотвращения угроз. Поэтому внедрение

новых внутренних регламентов в разрабатываемую методику предотвращения угроз является целесообразным для обеспечения более высокого уровня защиты информационной безопасности.

В первую очередь, необходимо внедрить регламент по проведению регулярного мониторинга угроз информационной безопасности на АРМ предприятия, поскольку качественное проведение мониторинга может существенно снизить количество возможных угроз. Мониторинг также может способствовать предотвращению возникновения угроз информационной безопасности технического характера. Данный регламент должен содержать следующие основные положения, которые будут осуществляться еженедельно:

- проведение мониторинг специалистом отдела информационной безопасности предприятия АРМ с помощью установленных программных продуктов;
- создание регулярной системы отчетности по мониторингу действующих АРМ;
- проведение тестовых опросов состояния оборудования;
- выполнение тестовых запросов к ИС и электронным сервисам и анализ полученных ответов;
- проведение анализа данных журналов операций, регистрируемых ИС Инфраструктуры взаимодействия;
- при выявлении в результате мониторинга фактов недоступности электронных сервисов, информационной системы, сбоев в функционировании оборудования специалист отдела информационной безопасности регистрирует инцидент, заводит обращение, определяет его приоритет и направляет его Участнику взаимодействия, в зоне ответственности которого возник инцидент;

– специалист отдела информационной безопасности размещает и обновляет результаты мониторинга электронных сервисов и статистику обращений к ним.

Помимо регламента по проведению мониторинга, необходимо внедрение регламента по проведению корреляции событий безопасности. Данный регламент подразумевает процесс выявления последовательности разнородных событий безопасности, имеющих логическую связь, которые могут быть значимы для выявления возможных нарушений безопасности информации. Основными задачами использования регламента корреляции являются:

1. Снижение объема исходного потока событий безопасности за счет группирования взаимосвязанных событий, что позволяет снизить когнитивную нагрузку на аналитика.
2. Определение взаимосвязей между событиями от разнородных источников, что способствует лучшему пониманию развития атаки в информационной системе.
3. Корреляция событий в контексте системы, что позволяет лучше понять сценарий атаки, ее цели и задачи.

Существуют различные схемы классификации разработанных методик корреляции событий, незначительно отличающиеся друг от друга. Можно выделить три основные группы исходя из их особенностей реализации и решаемых с их помощью задач корреляции:

– на основе сходства событий безопасности;
– на основе знаний;
– вероятностные или статистические.

Также необходимо внедрение регламента по реагированию на инциденты информационной безопасности, который включает следующие основные этапы по работе с инцидентами:

– обнаружение инцидента ИБ;

- анализ исходной информации и принятие решения о проведении разбирательства;
- разбирательство инцидента информационной безопасности.

Разбирательство Инцидента ИБ, в свою очередь, состоит из следующих этапов:

- подтверждение или опровержение факта возникновения инцидента ИБ;
- классификация инцидента ИБ;
- подтверждение/корректировка уровня значимости инцидента ИБ;
- уточнение дополнительных обстоятельств (деталей) инцидента ИБ;
- получение (сбор) доказательств возникновения инцидента ИБ, обеспечение их сохранности и целостности; минимизация последствий инцидента ИБ;
- информирование и консультирование персонала организации по действиям обнаружения.

4. Устранения последствий и предотвращения инцидентов ИБ.
5. Переоценка рисков, повлекших возникновение инцидента, актуализация необходимы.
6. Оформление результатов проведённого анализа.

Помимо внедрения регламентов информационной безопасности, необходимо регулярное проведение следующих мероприятий:

- повышение эффективности системы подготовки кадров. Проведение специализированного обучения сотрудников информационной безопасности по работе с выявлением и предотвращением угроз информационной безопасности;
- проведение регулярного контроля за принимаемыми мерами по обеспечению безопасности информации и уровня защищенности информационных систем;

– создание и ведение внутреннего журнала учета по использованию машинных носителей с фиксацией информации о времени, сотруднике и отделе.

Необходимо отметить, что действующая система информационной безопасности предприятия также нуждается во внедрении нового программного продукта, обеспечивающего информационную безопасность, поскольку действующий программный продукт имеет существенный ряд недостатков, которые были проанализированы ранее. Программный продукт будет являться инструментом обеспечения информационной безопасности предприятия. Программный продукт необходим при столкновении со следующими сложностями на предприятии:

– возможность утечки конфиденциальной информации или государственной тайны;
– несоответствие уровня обеспечения безопасности на предприятия нормам законодательства;
– возможность кражи конфиденциальной информации с целью получения коммерческой выгоды.

Проведем анализ программы «Блокхост-Сеть 2.0» для определения соответствия необходимым требованиям предприятия. В первую очередь, необходимо рассмотреть механизмы защиты, которыми располагает исследуемая программа.

К механизмам защиты относятся [41]:

– двухфакторная аутентификация пользователей с помощью электронных носителей ключевой информации;
– разграничение возможности доступа пользователей к папкам и файлам, включая временное ограничение;
– контроль и ограничение запуска процессов;
– контроль вывода информации на внешние жесткие диски и флэш-накопители;

– контроль изменения реестра и его восстановление.

Таким образом, можно выделить ряд преимуществ внедрения программы «Блокхост-Сеть 2.0». Необходимо отметить, что программа лицензирована и имеет необходимую сертификацию, способна обеспечить соответствие требованиям законодательства. Программа характеризуется централизованным развертыванием и обновлением средств защиты информации, а также удобна в администрировании [41].

В заключении, необходимо отметить, что выбранная программа полностью соответствует установленным требованиям и нормам предприятия. Имеет 3 класс защищенности в соответствии с руководящим документом «Средства вычислительной техники. Защита от несанкционированного доступа к информации», 2 уровень контроля недекларированных возможностей и 4 класс защищенности в соответствии с документом «Средства вычислительной техники. Показатели защищенности от несанкционированного доступа к информации» [41].

3.3 План внедрения СЗИ от НДС «Блокхост-сеть 2.0»

На данный момент контроль за соблюдением сотрудниками требований безопасности при работе с защищаемыми ресурсами с использованием АРМ осуществляется сотрудниками организации, которые сообщают о замеченных ими нарушениях в отдел информационной безопасности. По этим сообщениям проводится проверка соблюдения требований ИБ.

Данный подход имеет следующие недостатки:

1. Подверженность человеческому фактору: сотрудник может не обратить внимание на нарушение требований ИБ, не оценить в полной мере опасность нарушения, проигнорировать его, забыть сообщить о нарушении или сделать это несвоевременно.
2. Отсутствие непрерывного контроля: контроль осуществляется только при наличии вблизи АРМ, используемого для работы с защищаемыми

ресурсами, сотрудников отдела ИБ, которые могут наблюдать за работающим.

3. Большой расход рабочего времени сотрудников отдела ИБ на проведение проверок соблюдения требований ИБ на АРМ.
4. Функциональная схема осуществления контроля за соблюдением ИБ в нотации IDEF0 на данный момент показана на рисунке 17 (схема AS-IS).

Рисунок 17 – Модель AS-IS, нулевой уровень[19]

Далее изображена декомпозиция процесса осуществления контроля за соблюдением ИБ, которая включает выявление инцидента, установление обстоятельств по предотвращению инцидентов и принятие мер по предотвращению инцидентов.

[19] Составлено автором по: [49,59]

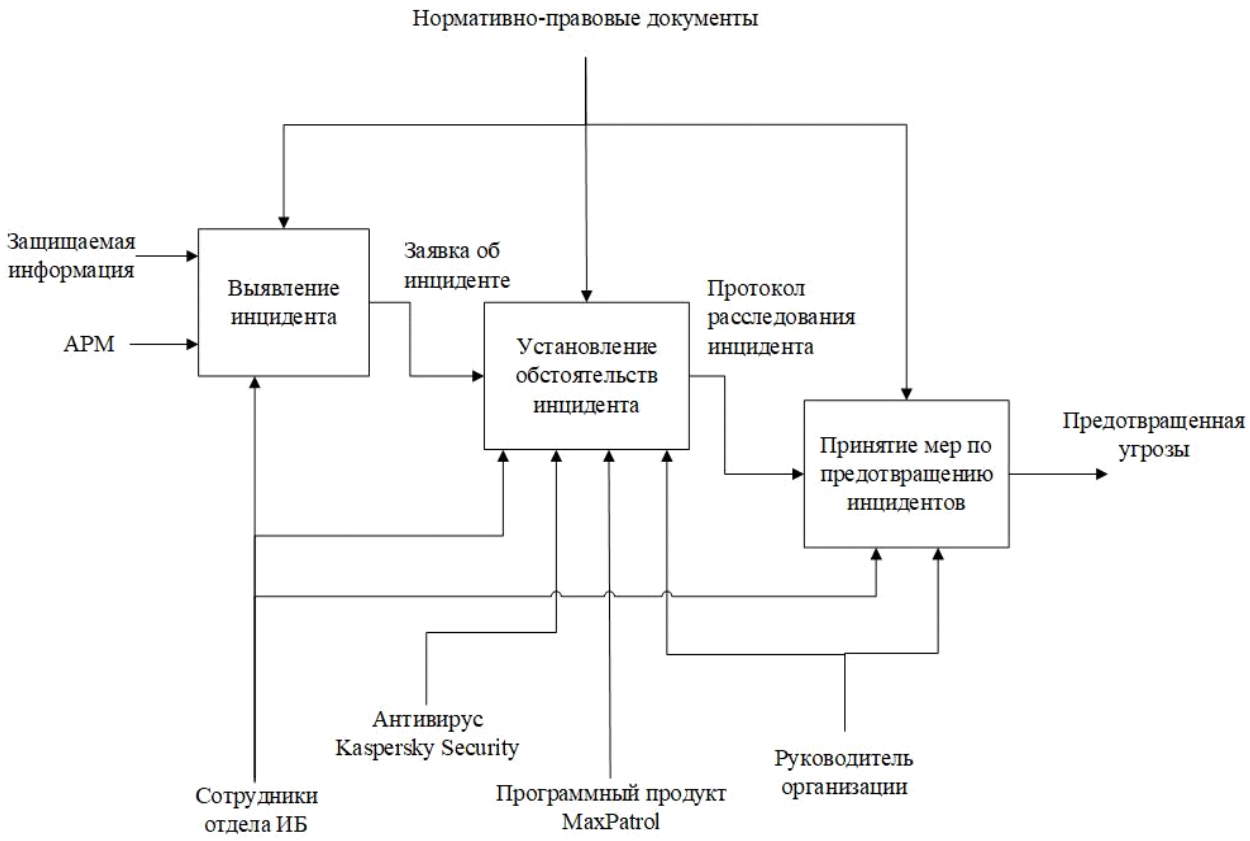


Рисунок 18 – Модель AS-IS, первый уровень[20]

Таким образом, можно сделать вывод, что процесс выявления угроз информационной безопасности на предприятии недостаточно эффективен. Далее будет описан измененный процесс выявления и предотвращения угроз.

Общий процесс контроля за соблюдением информационной безопасности не подвергся глобальным изменениям, однако внедрение программного продукта «Блокхост-Сеть 2.0» внесло определенные корректировки процесса.

[20] Составлено автором по: [49,59]

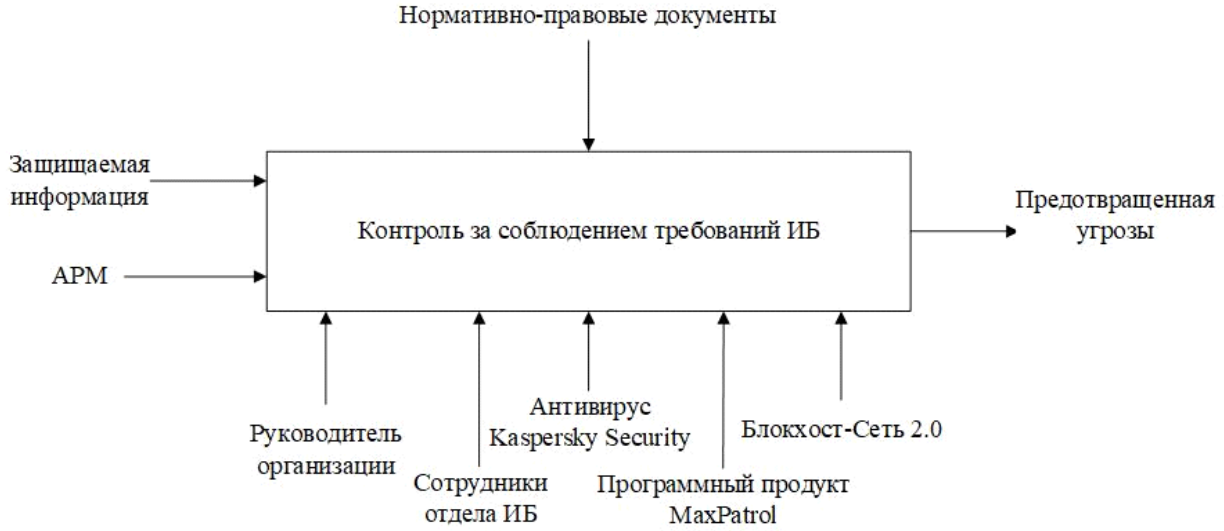


Рисунок 19 – Модель TO-BE, нулевой уровень[21]

Внедрение программного продукта «Блокхост-Сеть 2.0» позволяет снизить уровень воздействия человеческого фактора на осуществление контроля за соблюдением требований ИБ, также эксплуатация данной программы позволит обеспечить непрерывный контроль за АРМ, что может существенно сократить нерациональное использование рабочего времени на проверку соблюдения требований, а также повысить эффективность работы отдела информационной безопасности предприятия.

Далее представлен процесс осуществления контроля соблюдения информационной безопасности после внедрения программы «Блокхост-Сеть 2.0».

[21] Составлено автором по: [49,59]

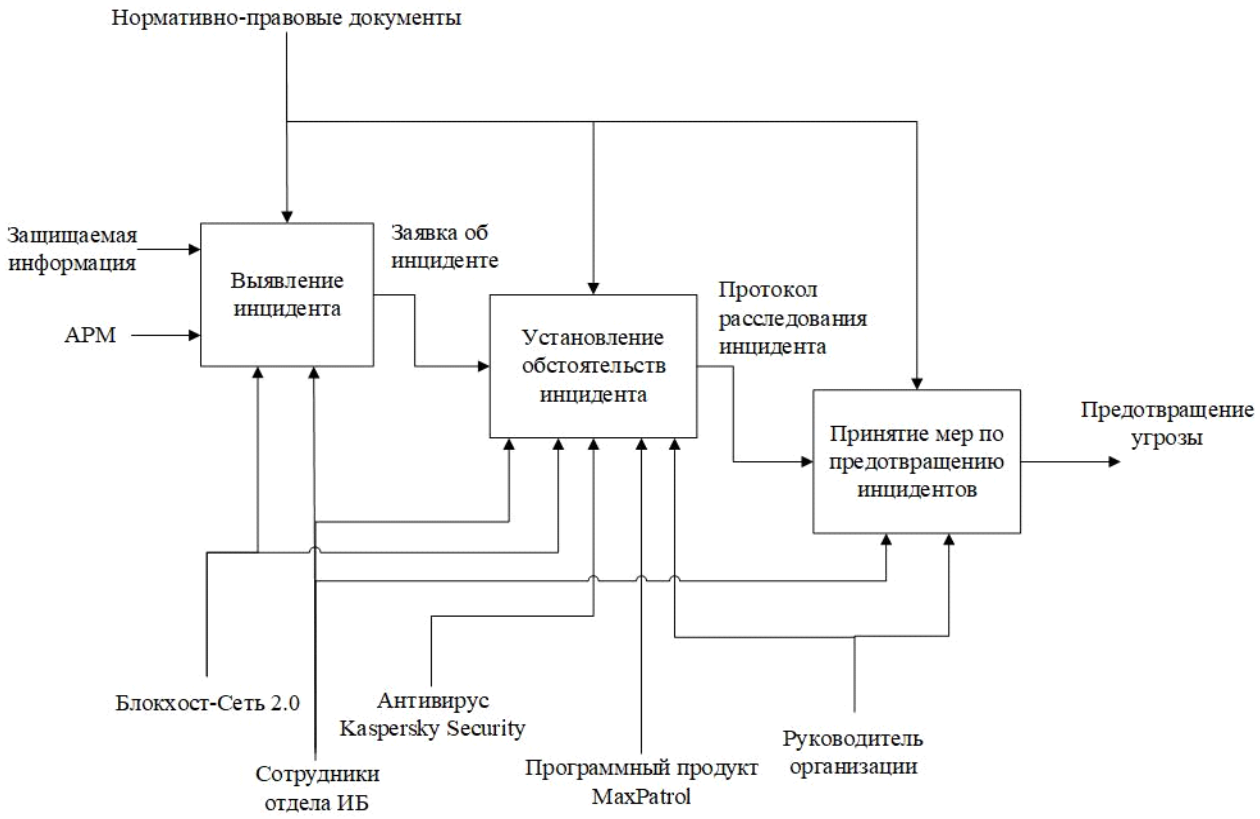


Рисунок 20 – Модель TO-BE, первый уровень[22]

3.4 Проект внедрения предотвращения угроз в MS Project

3.4.1 Сетевая модель

Внедрение методики предотвращения угроз ИБ в ФНС осуществляется в соответствии со стандартом PMBOK, в котором формализируются, стандартизируются и структурируются форматы проектной деятельности, описываются подходы к организации и концепции управления проектами. Основной областью знаний стандарта является управление интеграцией.

Интеграция процессов управления проектом — это взаимосвязи групп процессов и входящих в них процессов, обеспечивающие непрерывный и комплексный подход к управлению проектной деятельностью.

Управление интеграцией включает все пять групп процессов:

[22] Составлено автором по: [49,59]

- концепция (инициализация);
- планирование;
- исполнение;
- управление и контроль
- завершение.

Ниже приводится краткое описание работ выбранного стандарта.

a) Концепция проекта:
    1) Формулировка целей и задач;
    2) Анализ организации;
    3) Разработка плана внедрения;
    4) Формирование команды проекта;
    5) Оценка рисков проекта;
    6) Согласование и утверждение плана.
b) Планирование проекта:
    1) Планирование сроков длительности проекта;
    2) Планирование бюджет проекта;
    3) 10. Ознакомление с требованиями регламентов;
    4) 11. Утверждение плана финансирования;
    5) 11. Подготовка и утверждение технического задания;
    6) 12. Заключение договора.
c) Реализация (исполнение) проекта:
    1) 13. Предоставление регламентов
    2) 14. Настройка аутентификации пользователей;
    3) 15. Обеспечение доступа АРМ к серверу администрирования;
    4) 15. Проведение обучающих мероприятий для сотрудников;
    5) 16. Предоставление обучающих материалов, инструкций;
    6) 17. Выполнение процедур тестирования.
d) Управление и контроль проекта
    1) 18. Запуск программы в тестовом режиме;

2) 19. Подготовка пользовательских инструкций;
3) 20. Настройка отчетов по анализу внедрения;
4) 21. Выполнение процедур верификации.

е) Завершение проекта

1) 22. Запуск методики в эксплуатацию;
2) 23. Опытная эксплуатация;

Итог: 23 работы в проекте.

На сетевом графике представлено, что проект состоит из 5 этапов и 23 работ.

Ряд работ можно выполнять как последовательно, так и параллельно друг другу. Можно также расчленять работу на параллельно выполняемые операции для сокращения времени ее выполнения. Последовательность выполнения работ представлена ниже.

Работа «Анализ организации» следует после работы «Формулировка целей и задач». Из работы «Анализ организации» вытекают 3 процесса: «Оценка рисков проекта», «Формирование команды проекта», «Разработка плана внедрения». Далее из 3 предыдущих работ следует «Согласование плана».

Затем идут параллельно работы «Планирование сроков длительности проекта», «Планирование бюджета проекта» «Ознакомление с требованиями регламентов». «Утверждение плана финансирования» и «Подготовка и утверждение технического задания» вытекают из работы «Планирование бюджета проекта» и входят в «Заключение договора». Сетевая модель представлена на рисунке 21.

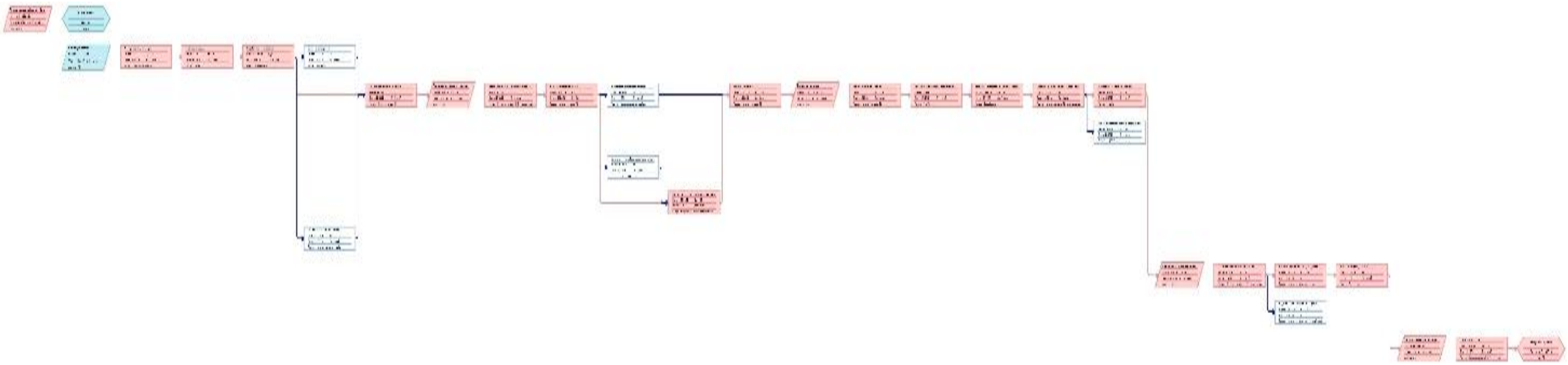


Рисунок 21 – Сетевая модель[23]

[23] Составлено автором по: [61]

3.4.2 Календарное планирование

Календарный план демонстрирует разделение проектного задания на этапы. Данный план содержит упорядоченную по времени последовательность работ проекта. Это позволяет руководству планировать деятельность сотрудников предприятия.

Наименование работ указаны на рисунке 22.

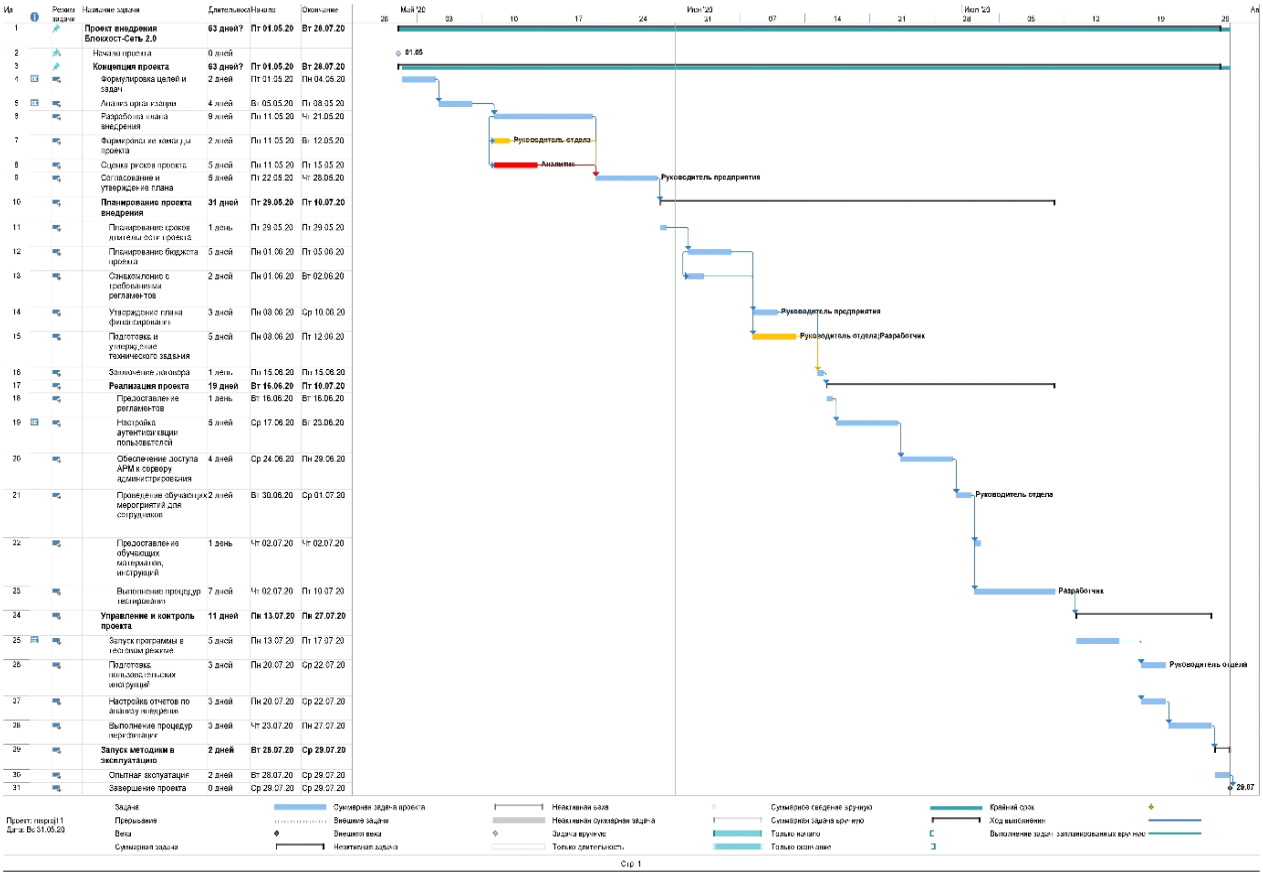
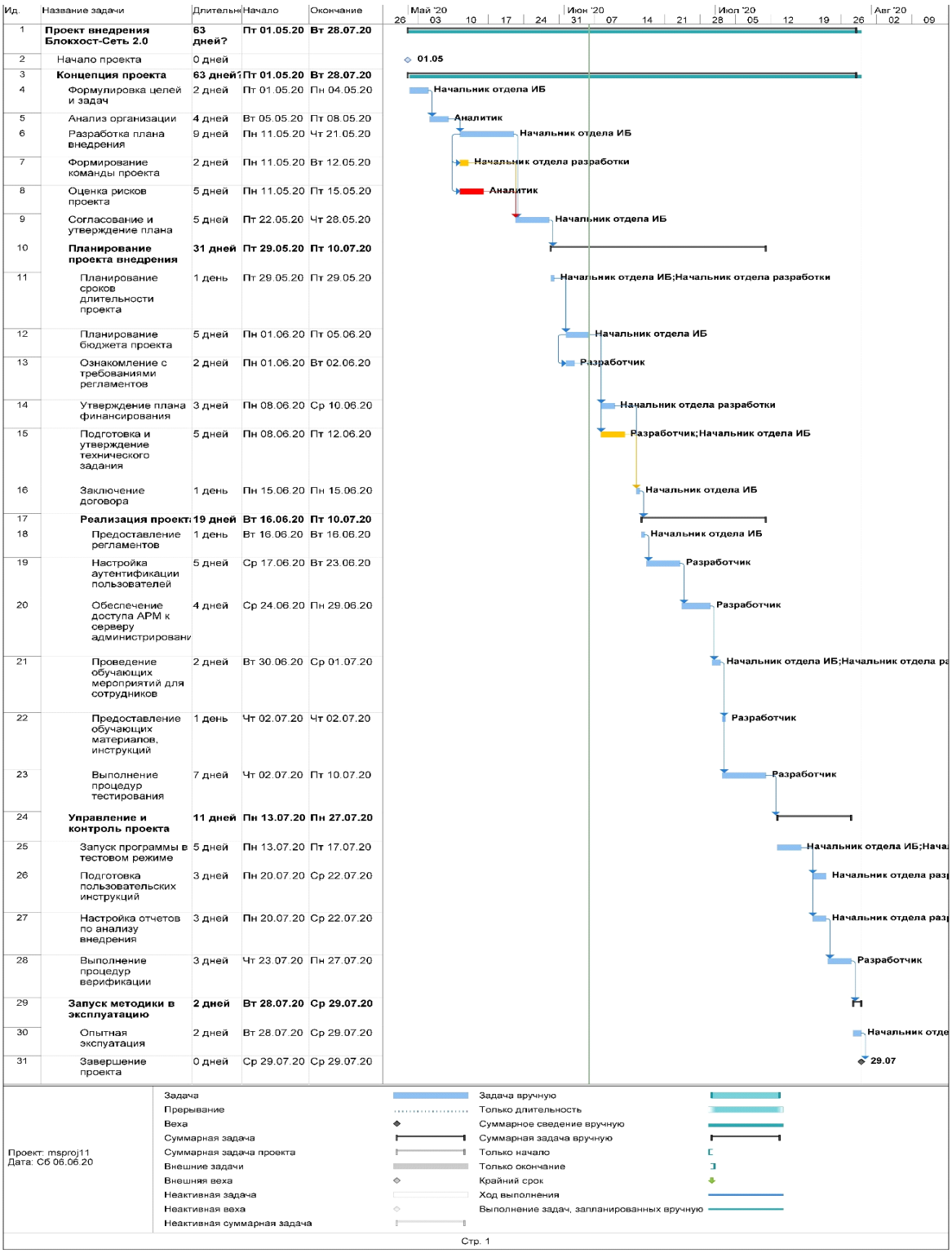


Рисунок 22 – Диаграмма Ганта[24]

Продолжительность всего проекта составляет 63 рабочих дня.

[24] Составлено автором по: [18]



Ид.	Название задачи	Длительн	Начало	Окончание
1	**Проект внедрения Блокхост-Сеть 2.0**	**63 дней?**	**Пт 01.05.20**	**Вт 28.07.20**
2	Начало проекта	0 дней		
3	**Концепция проекта**	**63 дней?**	**Пт 01.05.20**	**Вт 28.07.20**
4	Формулировка целей и задач	2 дней	Пт 01.05.20	Пн 04.05.20
5	Анализ организации	4 дней	Вт 05.05.20	Пт 08.05.20
6	Разработка плана внедрения	9 дней	Пн 11.05.20	Чт 21.05.20
7	Формирование команды проекта	2 дней	Пн 11.05.20	Вт 12.05.20
8	Оценка рисков проекта	5 дней	Пн 11.05.20	Пт 15.05.20
9	Согласование и утверждение плана	5 дней	Пт 22.05.20	Чт 28.05.20
10	**Планирование проекта внедрения**	**31 дней**	**Пт 29.05.20**	**Пт 10.07.20**
11	Планирование сроков длительности проекта	1 день	Пт 29.05.20	Пт 29.05.20
12	Планирование бюджета проекта	5 дней	Пн 01.06.20	Пт 05.06.20
13	Ознакомление с требованиями регламентов	2 дней	Пн 01.06.20	Вт 02.06.20
14	Утверждение плана финансирования	3 дней	Пн 08.06.20	Ср 10.06.20
15	Подготовка и утверждение технического задания	5 дней	Пн 08.06.20	Пт 12.06.20
16	Заключение договора	1 день	Пн 15.06.20	Пн 15.06.20
17	**Реализация проект**	**19 дней**	**Вт 16.06.20**	**Пт 10.07.20**
18	Предоставление регламентов	1 день	Вт 16.06.20	Вт 16.06.20
19	Настройка аутентификации пользователей	5 дней	Ср 17.06.20	Вт 23.06.20
20	Обеспечение доступа АРМ к серверу администрировани	4 дней	Ср 24.06.20	Пн 29.06.20
21	Проведение обучающих мероприятий для сотрудников	2 дней	Вт 30.06.20	Ср 01.07.20
22	Предоставление обучающих материалов, инструкций	1 день	Чт 02.07.20	Чт 02.07.20
23	Выполнение процедур тестирования	7 дней	Чт 02.07.20	Пт 10.07.20
24	**Управление и контроль проекта**	**11 дней**	**Пн 13.07.20**	**Пн 27.07.20**
25	Запуск программы в тестовом режиме	5 дней	Пн 13.07.20	Пт 17.07.20
26	Подготовка пользовательских инструкций	3 дней	Пн 20.07.20	Ср 22.07.20
27	Настройка отчетов по анализу внедрения	3 дней	Пн 20.07.20	Ср 22.07.20
28	Выполнение процедур верификации	3 дней	Чт 23.07.20	Пн 27.07.20
29	**Запуск методики в эксплуатацию**	**2 дней**	**Вт 28.07.20**	**Ср 29.07.20**
30	Опытная экспуатация	2 дней	Вт 28.07.20	Ср 29.07.20
31	Завершение проекта	0 дней	Ср 29.07.20	Ср 29.07.20

Рисунок 23 – Диаграмма Ганта[25]

[25] Составлено автором по: [18]

3.5 Обоснование экономической эффективности проекта

3.5.1 Стоимостное планирование проекта

Экономический подраздел выпускной квалификационной работы содержит экономическое обоснование проекта внедрения программного продукта, которое является средством защиты информации от несанкционированного доступа «Блокхост – Сеть 2.0» для автоматизации бизнес-процесса выявления и своевременное предотвращение угроз информационной безопасности территориального налогового органа.

Расчет вложений на этапе внедрения программного продукта

На этапе внедрения со стороны предприятия участвует: начальник отдела информационной безопасности (ИБ), заместитель начальника отдела ИБ, главный специалист-эксперт, ведущий специалист-эксперт, специалист первого разряда. Работы по проекту внедрения выполняют: начальник отдела информационной безопасности, аналитик, разработчик. Стоимость часа работы на этапе финансирования приведена в Таблице 3. Справочные величины по использованным в расчетах налогам и страховым взносам приведены в Таблице 4. Внедрение длится 63 дня. Расчет затрат на оплату труда на этапе внедрения приведен в Таблице 5.

Таблица 3. Стоимость часа работы на этапе внедрения[26]

Должность специалиста	**Зарплата "на руки", руб./мес.**	**НДФЛ, руб./мес.**	**Зарплата "на руки" +НДФЛ, руб./мес.**	**Страховые взносы, руб./мес.**	**Затраты на оплату труда, руб./мес.**	**Затраты на оплату труда, руб./ч**
Начальник отдела ИБ	16 000	2 390,80	18 390,80	5 554,02	23 944,83	**143**
Заместитель начальника отдела ИБ	15 000	2 241,38	17 241,38	5 206,90	22 448,28	**134**
Главный специалист-эксперт	14 000	2 091,95	16 091,95	4 859,77	20 951,72	**125**
Ведущий специалист-	13 000	1 942,53	14 942,53	4 512,64	19 455,17	**116**

[26] Составлено автором по: [62]

эксперт						
Специалист первого разряда	12 000	1 793,10	13 793,10	4 165,52	17 958,62	**107**
Начальник отдела разработки	17 000	2 540,23	19 540,23	5 901,15	25 441,38	**151**
Аналитик	15 500	2 316,09	17 816,09	5 380,46	23 196,55	**138**
Разработчик	14 500	2 166,67	16 666,67	5 033,33	21 700,00	**129**

Таблица 4. Справочные величины по налогам и страховым взносам[27]

Ставка НДФЛ	**13%**
Страховые взносы, в том числе	**30,2%**
Пенсионное страхование	22,0%
Медицинское страхование	5,1%
Социальное страхование	2,9%
Взносы на травматизм	0,2%

Таблица 5. Расчетное количество часов[28]

Кол-во рабочих часов в месяце	**168**
Кол-во рабочих дней в месяце	21
Кол-во рабочих часов в день	8

Таблица 6. Затраты на оплату труда на этапе финансирования[29]

Этап проекта/Специалист	**Трудозатраты, ч**	**Ставка, руб./ч**	**Затраты на опл. труда, руб.**
Концепция проекта	**216**		**30 656**
Начальник отдела ИБ	128	143	18 304
Начальник отдела разработки	16	151	2 416
Аналитик	72	138	9 936
Планирование проекта внедрения			**25 784**
Начальник отдела ИБ	96	143	13 728
Начальник отдела разработки	32	151	4 832

[27] Составлено автором по: [62]
[28] Составлено автором по: [62]
[29] Составлено автором по: [62]

Разработчик	56	129	7 224
Реализация проекта	**176**		**23 392**
Начальник отдела ИБ	24	143	3 432
Начальник отдела разработки	16	151	2 416
Разработчик	136	129	17 544
Управление и контроль проекта	**176**		**25 200**
Начальник отдела ИБ	40	143	5 720
Начальник отдела разработки	88	151	13 288
Разработчик	48	129	6 192
Запуск методики в эксплуатацию	**32**		**4 352**
Начальник отдела ИБ	16	143	2 288
Разработчик	16	129	2 064
		ИТОГО:	**109 384**

Нематериальные вложения, которые потребуются на этапе внедрения, представлены в Таблице 7 соответственно.

Для размещения программного продукта «Блокхост – сеть 2.0» предназначен персональный компьютер, который одновременно является рабочим местом в серверной. Клиентские лицензии для автоматизированных рабочих мест сотрудников предприятия.

Таблица 7. Нематериальные вложения на этапе внедрения[30]

№	Категории и статьи вложений	Кол-во	Цена, руб. без НДС	Стоимость, руб. без НДС
II	**Нематериальные вложения**			**420 000**
A	**Лицензии на программное обеспечение**			**420 000**
1	Серверная лицензия Блок-хост 2.0	1	120 000	120 000
2	Клиентские лицензии	300	1 000	300 000

Нематериальные вложения включают в себя СЗИ от НСД «Блокхост – сеть 2.0» для автоматизации выявления угроз информационной безопасности на 300 рабочих мест – после внедрения программного продукта угрозы информационной безопасности можно автоматически выгружать в форме

[30] Составлено автором по: [62]

отчета. Клиентские лицензии для соединения с сервером администрирования программного продукта «Блокхост – сеть 2.0» и рабочими станциями всех сотрудников предприятия.

Накладные расходы на этапе внедрения приведены в Таблице 7. Для расчета взят принятый на предприятии процент накладных расходов от суммы затрат на оплату труда задействованных в проекте специалистов.

Таблица 8. Накладные расходы на этапе внедрения[31]

№	Статьи накладных расходов	Содержание статей накладных расходов
1	Рабочее место	Помещение, уборка, электроэнергия, мебель
2	Управленческие расходы	Руководство компании + бухгалтерия
3	Канцелярские товары	Офисная бумага, маркеры, папки
	Метод расчета накладных расходов	**[% от трудозатрат в денежных единицах]**
[A]	Сумма трудозатрат в денежных единицах (руб.)	**109 384**
[B]	Принятая доля (%) накладных расходов от [A]	**15%**
[C]	Накладные расходы в денежных единицах (руб.)	**16 408**

3.5.2 Структура и денежная оценка

На этапе эксплуатации проекта поддержку внедренного программного продукта по обеспечению информационной безопасности со стороны предприятия выполняют начальник отдела разработки. Внешний исполнитель по договору на сервисное обслуживание внедренной системы обеспечивает ее бесперебойную работу. Затраты на оплату труда начальника отдела и специалистов отдела, а также на бумагу и расходные материалы для их деятельности, учтены при расчете экономического эффекта от внедрения.

Стоимость часа работы на этапе эксплуатации приведена в Таблице 9. Справочные величины по использованным в расчетах налогам и страховым взносам приведены в Таблице 4. Эксплуатация осуществляется на

[31] Составлено автором по: [62]

регулярной основе. Расчет затрат на оплату труда на этапе эксплуатации из расчета на один месяц приведен в Таблице 9.

Таблица 9. Стоимость часа работы на этапе эксплуатации[32]

Должность специалиста	**Зарплата "на руки", руб./мес.**	**НДФЛ, руб./мес.**	**Зарплата "на руки" +НДФЛ, руб./мес.**	**Страховые взносы, руб./мес.**	**Затраты на оплату труда, руб./мес.**	**Затраты на оплату труда, руб./ч**
Начальник отдела ИБ	16 000	2 390,80	18 390,80	5 554,02	23 944,83	**143**
Заместитель начальника отдела ИБ	15 000	2 241,38	17 241,38	5 206,90	22 448,28	**134**
Главный специалист-эксперт	14 000	2 091,95	16 091,95	4 859,77	20 951,72	**125**
Ведущий специалист-эксперт	13 000	1 942,53	14 942,53	4 512,64	19 455,17	**116**
Специалист первого разряда	12 000	1 793,10	13 793,10	4 165,52	17 958,62	**107**
Начальник отдела разработки	17 000	2 540,23	19 540,23	5 901,15	25 441,38	**151**
Аналитик	15 500	2 316,09	17 816,09	5 380,46	23 196,55	**138**
Разработчик	14 500	2 166,67	16 666,67	5 033,33	21 700,00	**129**

[32] Составлено автором по: [62]

Таблица 10. Затраты на оплату труда на этапе эксплуатации (ежемесячно)[33]

Этап проекта/Специалист	**Трудозатраты, ч**	**Ставка, руб./ч**	**Затраты на опл. труда, руб.**
Начальник отдела ИБ	3	143	429
Заместитель начальника отдела ИБ	6	134	804
Главный специалист-эксперт	25	125	3125
		ИТОГО:	**4 358**

Накладные расходы на этапе эксплуатации приведены в Таблице 11. Для расчета взят принятый на предприятии – процент накладных расходов от суммы затрат на оплату труда задействованных в проекте специалистов (в данном проекте на этапе эксплуатации.

Таблица 11. Накладные расходы на этапе эксплуатации (ежемесячно)[34]

№	**Статьи накладных расходов**	**Содержание статей накладных расходов**
1	Рабочее место	Помещение, уборка, электроэнергия, мебель
2	Управленческие расходы	Руководство компании + бухгалтерия
3	Канцелярские товары	Офисная бумага, маркеры, папки
	Метод расчета накладных расходов	**[% от трудозатрат в денежных единицах]**
[A]	Сумма трудозатрат в денежных единицах (руб.)	**4 358**
[B]	Принятая доля (%) накладных расходов от [A]	**15%**
[C]	Накладные расходы в денежных единицах (руб.)	**654**

Экономический эффект от реализации проекта для выбранного предприятия заключается в уменьшении рабочего времени сотрудников отдела безопасности, которое сотрудники тратят на выявление и предотвращение угроз информационной безопасности предприятия. Для оценки эффекта взята разница в стоимости процесса «AS-IS» и «TO-BE» во

[33] Составлено автором по: [62]
[34] Составлено автором по: [62]

времени нахождения и предотвращения угроз. Расчет стоимости выполнен с помощью метода функционально стоимостного анализа (далее ФСА).

Для реализации ФСА в Таблице 12 приведена стоимость часа работы специалистов отдела информационной безопасности.

Таблица 12. Стоимость часа работы при использовании "Блокхост-сеть 2.0"[35]

Должность специалиста	**Зарплата "на руки", руб./мес.**	**НДФЛ, руб./мес.**	**Зарплата "на руки" +НДФЛ, руб./мес.**	**Страховые взносы, руб./мес.**	**Затраты на оплату труда, руб./мес.**	**Затраты на оплату труда, руб./ч**
Начальник отдела ИБ	16 000	2 390,80	18 390,80	5 554,02	23 944,83	143
Заместитель начальника отдела ИБ	15 000	2 241,38	17 241,38	5 206,90	22 448,28	134
Главный специалист-эксперт	14 000	2 091,95	16 091,95	4 859,77	20 951,72	125
Ведущий специалист-эксперт	13 000	1 942,53	14 942,53	4 512,64	19 455,17	116
Специалист первого разряда	12 000	1 793,10	13 793,10	4 165,52	17 958,62	107
Начальник отдела разработки	17 000	2 540,23	19 540,23	5 901,15	25 441,38	151
Аналитик	15 500	2 316,09	17 816,09	5 380,46	23 196,55	138
Разработчик	14 500	2 166,67	16 666,67	5 033,33	21 700,00	129

В таблице 13 приведен расчет затрат на оплату труда специалистов отдела предприятия, задействованных в обеспечении информационной безопасности «AS-IS» и «TO-BE». Расчет основан на почасовых ставках из Таблицы 10 и количества часов в месяц, затрачиваемых сотрудниками в период эксплуатации программного продукта «Блокхост – сеть 2.0». «AS-IS» и «TO-BE» в отделе информационной безопасности предприятия задействованы все сотрудники отдела. Ожидается, что внедрение данного программного продукта для автоматизации выявления и предотвращения угроз информационной безопасности позволит уменьшить количество часов

[35] Составлено автором по: [62]

работы над данным процессом работников отдела информационной безопасности.

Таблица 13. Затраты на оплату труда отдела информационной безопасности «AS-IS» и «TO-BE»[36]

Этап проекта/Специалист	Ставка, руб./ч	«AS-IS»		«TO-BE»	
		Трудозатраты, ч	Затраты на опл. труда, руб.	Трудозатраты, ч	Затраты на опл. труда, руб.
Руководство процессом контроля			**2 574**		**286**
Начальник отдела ИБ	**143**	**18**	**2 574**	**2**	**286**
Распределение задач между сотрудниками			**4 690**		**402**
Заместитель начальника отдела ИБ	**134**	**35**	**4 690**	**3**	**402**
Выявление нарушений			**12 250**		**625**
Главный специалист-эксперт	**125**	**98**	**12 250**	**5**	**625**
Выявление нарушений			**18 444**		**812**
Ведущий специалист-эксперт	**116**	**159**	**18 444**	**7**	**812**
Выявление нарушений			**17 120**		**749**
Специалист первого разряда	**107**	**160**	**17 120**	**7**	**749**

3.5.3 Расчет показателей эффективности и их оценка

Для оценки экономической эффективности внедрения программного продукта «Блокхость-Сеть 2.0» для автоматизации мониторинга угроз информационной безопасности рассчитаны финансовые показатели NPV (Net Present Value) – чистый приведенный доход, IRR (Internal Rate of Return) - внутренняя норма доходности, DPP (Discounted Payback Period) – срок окупаемости с учетом дисконтирования. Сводная информация для расчета финансовых показателей приведена в Таблице 14.

[36] Составлено автором по: [62]

Ставка дисконтирования выбрана в размере 9% годовых из расчета безрисковой ставки 6% годовых (ключевая ставка Банка России на 15.03.2020) плюс 3% годовых платы за риск (экспертная оценка специалистов заказчика).

Расчеты выполнены помесячно (период 16 мес.). Ставка дисконтирования:

$$R_{\text{мес}} = \sqrt[12]{1 + R_{\text{год}}} - 1 = 0{,}7207\% \quad (1)$$

Коэффициент дисконтирования:

$$K_{\text{дисконт}}^{1-\text{й год}} = 1/(1 + R_{\text{мес}})^{12} = 0{,}9174,\ K_{\text{дисконт}}^{2-\text{й год}} = 1/(1 + R_{\text{мес}})^{24} = 0{,}8417 \quad (2)$$

Налог на прибыль взят в размере 20% для предприятия с общей системой налогообложения. Все показатели учтены без НДС. Амортизация не учитывается.

Таблица 14. Сводная информация для расчета финансовых показателей[37]

	Этап	Этап эксплуатации														руб.
	финансирования	1-й мес.	2-й мес.	3-й мес.	4-й мес.	5-й мес.	6-й мес.	7-й мес.	8-й мес.	9-й мес.	10-й мес.	11-й мес.	12-й мес.	13-й мес.	14-й мес.	15-й мес.	16-й мес.
1. Инвестиционные и текущие вложения (отток ДС)	**545 792**	**5 012**	**5 012**	**5 012**	**5 012**	**5 012**	**5 012**	**5 012**	**5 012**	**5 012**	**5 012**	**5 012**	**5 012**	**5 012**	**5 012**	**5 012**	**5 012**
Расходы на оплату труда	109 384	4 358	4 358	4 358	4 358	4 358	4 358	4 358	4 358	4 358	4 358	4 358	4 358	4 358	4 358	4 358	4 358
Нематериальные вложения	420 000																
Накладные расходы	16 408	654	654	654	654	654	654	654	654	654	654	654	654	654	654	654	654
2. Приток ДС	**0**	**52 204**	**52 204**	**52 204**	**52 204**	**52 204**	**52 204**	**52 204**	**52 204**	**52 204**	**52 204**	**52 204**	**52 204**	**52 204**	**52 204**	**52 204**	**52 204**
Экономический эффект от реализации проекта (разница между "AS-IS" и "TO-BE")	0	52 204	52 204	52 204	52 204	52 204	52 204	52 204	52 204	52 204	52 204	52 204	52 204	52 204	52 204	52 204	52 204
3. Прибыль и налоги																	
База для расчета налога на прибыль нарастающим итогом	-545 792	-498 599	-451 407	-404 215	-357 022	-309 830	-262 638	-215 446	-168 253	-121 061	-73 869	-26 676	20 516	67 708	114 901	162 093	209 285
Прибыль по периодам	0	0	0	0	0	0	0	0	0	0	0	0	20 516	47 192	47 192	47 192	47 192
Налог на прибыль по периодам	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**4 103**	**9 438**	**9 438**	**9 438**	**9 438**
4. Чистый денежный поток по периодам (NCF_i)	**-545 792**	**47 192**	**47 192**	**47 192**	**47 192**	**47 192**	**47 192**	**47 192**	**47 192**	**47 192**	**47 192**	**47 192**	**43 089**	**37 754**	**37 754**	**37 754**	**37 754**
5. Чистый дисконтированный денежный поток по периодам (NCF_i * к-т дисконтирования)	**-545 792**	**43 296**	**43 296**	**43 296**	**43 296**	**43 296**	**43 296**	**43 296**	**43 296**	**43 296**	**43 296**	**43 296**	**39 531**	**31 777**	**31 777**	**31 777**	**31 777**
6. Чистый приведенный доход NPV в динамике	**-545 792**	**-502 496**	**-459 200**	**-415 905**	**-372 609**	**-329 313**	**-286 017**	**-242 722**	**-199 426**	**-156 130**	**-112 835**	**-69 539**	**-30 008**	**1 769**	**33 546**	**65 322**	**97 099**

[37] Составлено автором по: [62]

3.5.4 Итоги

Экономический эффект от внедрения как разница между стоимостью процесса выявления угроз информационной безопасности «AS-IS» и «TO-BE» составляет:

52 204 руб./мес. = 55 078 руб./мес. - 2 874 руб./мес.

На основании данных Таблицы 14 вычислены значения финансовых показателей проекта внедрения программного продукта «Блокхост-Сеть 2.0» для автоматизации мониторинга угроз информационной безопасности:

- Прогнозируемое значение показателя NPV за 16 месяцев: 112 127 руб.
- Срок окупаемости с учетом дисконтирования DPP: 15 мес.
- Внутренняя норма доходности IRR за 16 месяцев: 15.67% годовых.

Анализ прогнозируемых финансовых показателей (NPV > 0, DPP < Тмакс, IRR > CC) показал, что проект является экономически эффективным.

ЗАКЛЮЧЕНИЕ

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, внедрением дополнительных регламентов, сокращения воздействия человеческого фактора и автоматизации труда.

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

В первой главе были исследованы теоретические аспекты угроз информационной безопасности, рассмотрены основные задачи обеспечения информационной безопасности предприятия, а также была проведена подробная классификация угроз информационной безопасности.

Были изучены основные источники угроз информационной безопасности, которые могут оказать негативное воздействие на работу территориальных налоговых органов. Данная часть исследования имеет принципиальную значимость, поскольку своевременная идентификация и классификация угроз информационной безопасности необходима для эффективного обеспечения защиты информационных ресурсов.

В процессе исследования теоретической части были использованы работы отечественных и зарубежных авторов, электронные ресурсы, а также

материалы, полученные в ходе участия в конференции «БИТ Безопасность информационных технологий – Урал 2020».

Во второй главе был произведен анализ нормативно-правовой базы, обеспечивающая информационную безопасность, были выявлены основные недостатки действующих методов выявления угроз информационной безопасности на предприятии, а также был произведен обзор наиболее актуальных угроз информационной безопасности предприятия и произведен расчет уровня их возможной реализации. Проведен анализ методики определения угроз безопасности информации в информационных системах ФСТЭК.

В третьей главе представлена характеристика Федеральной налоговой службы и рассмотрена деятельность предприятия, сформированы следующие модели:

- взаимосвязь миссий, целей и задач;
- взаимосвязь стратегических целей и задач;
- ключевые факторы успеха для реализации стратегии;
- взаимосвязь бизнес-процессов и бизнес-функций;
- организационная структура компании;
- услуги ФНС России;
- архитектура приложений;
- связь приложений и функций;
- ИТ-инфраструктура.

Предложены основные направления модернизации методики определения угроз безопасности информации в информационных системах ФСТЭК.

Была проведена разработка комплексного плана мероприятий, направленного на сокращение угроз информационной безопасности. Установлена необходимость внедрения в процесс работы дополнительных регламентов: проведения регулярных мониторингов, проведения корреляции

событий безопасности, реагирования на инциденты. Были сформированы основные положения каждого из регламентов.

Была создана модель AS-IS, в которой была выделена проблема неэффективных процессов выявления и предотвращения угроз информационной безопасности, а также разработана модель TO-BE, оптимизирующая процессы с помощью внедрения программного продукта «БЛОКХОСТ-СЕТЬ 2.0».

Был спланирован проект внедрения оптимизации процесса предотвращения угроз информационной безопасности с помощью MS Project. Общая продолжительность проекта занимает 63 рабочих дня.

Подведены итоги с помощью расчета экономических показателей, которые продемонстрировали рентабельность и эффективность внедрения проекта.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. ГОСТ Р 50922-96 «Защита информации. Основные термины и определения»
2. Стрельцов А.А. Содержание понятия «обеспечение информационной безопасности» // Информационное общество №4. С.12 2015
3. Доктрина информационной безопасности Российской Федерации (утв. Указом Президента РФ 05.12.2016 г. №646) [Электронный ресурс]// СПС «Консультант-Плюс». URL: http//www.consultant.ru/document/cons_doc_LAW_28679/ (дата обращения 12.03.2020);
4. Федеральный Закон «О персональных данных» от 27 июля 2006 года № 152 (принят 27.06.2006, действующая редакция);
5. Федеральный закон «Об информации, информационных технологиях и защите информации» от 27 июля 2006 года № 149 (принят 27.07.2006, действующая редакция);
6. Федеральный Закон «О безопасности» от 07 декабря 2010 года № 2446-1 (принят 07.12.2010, действующая редакция);
7. Федеральный Закон от 21 июля 1993 года «О государственной тайне» №5485-1 (принят 21.07.1993, действующая редакция);
8. Налоговой Кодекс Российской Федерации от 16 июля 1998 года, действующая редакция;
9. «Положение о Федеральной налоговой службе» от 30 сентября 2004 года, действующая редакция;
10. Ст. 7 Закона «О персональных данных» от 27 июля 2006 года № 152 (принят 27.06.2006, действующая редакция);
11. Ч. 1 ст. 24 Конституции РФ от 25 декабря 1993 года, действующая редакция;

12. Указ Президента РФ от 31 декабря 2015 N 683 «О стратегии национальной безопасности» (принят 27.12.2015, действующая редакция);

13. Ожегов С.И. Словарь русского языка. М., 1963 – [Электронный ресурс]. – https://search.rsl.ru/ru/record/01001596547 (дата обращения 25.04.2020);

14. Международный научный журнал «Символ науки» №10/2018 – [Электронный ресурс]. – https://os-russia.com/sn (дата обращения 20.04.2020);

15. Дашян М.С. Право информационных магистралей – Law of Information Highways: вопросы правового регулирования в сфере Интернет. М.: ВолтерсКлувер, 20171963 – [Электронный ресурс]. – http://www.telecomlaw.ru/monograph/Dashyan.pdf (дата обращения 28.04.2020);

16. Научный интернет журнал «Мир науки». Выпуск 6 – 2016 – [Электронный ресурс]. – https://mir-nauki.com/issues.html (дата обращения 21.04.2020);

17. Вихорев С.В. Классификация угроз информационной безопасности – [Электронный ресурс]. – http://www.cnews.ru/reviews/free/security (дата обращения 04.04.2020);

18. Галатенко В.А. Основы информационной безопасности. М., 2016. 264 с. – [Электронный ресурс]. – http://en.bookfi.net/book/584428 (дата обращения 16.03.2020);

19. Яремчук С.А. – [Электронный ресурс] – http://www.mirandaim.info/protection (дата обращения 11.04.2020);

20. Выписка из Основных направлений научных исследований в области обеспечения информационной безопасности Российской Федерации. – [Электронный ресурс] – http://www.scrf.gov.ru/security/information/document155/ (дата обращения 11.03.2020);

21. Теория государства и права: учебник / Российский университет дружбы народов, Юридический институт под ред. д.ю.н.,проф А.А. Клишаса. – М.: Статут, 2019. – [Электронный ресурс] –

http://www.consultant.ru/edu/student/download_books/book/teoriya_gosudarstva_i_prava_uchebnik/ (дата обращения 11.03.2020);

22. Конституция Российской Федерации от 12 декабря 1993 года (принята 12.12.1993, действующая редакция);

23. Газета Известия 27 декабря 2019 г. – [Электронный ресурс] – https://iz.ru/newspaper/no247-27-dekabria-2019-goda (дата обращения 26.03.2020);

24. Судебный Департамент при Верховном Суде РФ – [электронный ресурс] – www.cdep.ru (дата обращения 12.04.2020);

25. Уголовный Кодекс Российской Федерации, Статья 137 «Нарушение неприкосновенности частной жизни» от 24 мая 1996 года (принят 24.05.1996, действующая редакция);

26. Указ Президента РФ от 10 января 2000 года N 24 «О Концепции национальной безопасности Российской Федерации» Концепция информационной безопасности Федеральной налоговой службы (принят 10.01.2000, действующая редакция);

27. Методика определения угроз безопасности информации в информационных системах. Методический документ утвержден ФСТЭК России 2015 г. – [Электронный ресурс] – https://fstec.ru/component/attachments/download/812 (дата обращения 02.03.2020);

28. Министерство Финансов Электронный ресурс официальный сайт – [Электронный ресурс] – https://www.minfin.ru/ru/ (дата обращения 23.03.2020);

29. Официальный сайт ФНС России – [Электронный ресурс] – https:\\nalog.ru\ (дата обращения 22.03.2020);

30. Постановление Правительства РФ от 30 сентября 2004 года № 506 "Об утверждении Положения о Федеральной налоговой службе" (принят 30.09.2004, действующая редакция);

31. Государственного контракт от 10.08.2015 № 5-7-02/117 – [Электронный ресурс]–

https://zakupki.gov.ru/epz/contract/contractCard/document-info.html?reestrNumber=1782606282118000053 (дата обращения 12.04.2020);

32. Цифровая трансформация международной налоговой системы – [Электронный ресурс] – http://worldtaxes.ru/tsifrovaya-transformatsiya-mezhdunarodnoj-nalogovoj-sistemy (дата обращения 17.03.2020);

33. Селифанов В.В., Слонкина И.С., Юракова Я.В. Определение актуальных угроз безопасности информации в государственных информационных системах, используя Банк данных угроз // Наука. Технологии. Инновации: сборник научных трудов в 9 частях. -Новосибирск, 2016. - С. 69-71. – [Электронный ресурс] – https://cyberleninka.ru/article/n/metodika-avtomatizirovannogo-vyyavleniya-vzaimosvyazey-uyazvimostey-i-ugroz-bezopasnosti-informatsii-v-informatsionnyh-sistemah (дата обращения 27.04.2020);

34. Гацко М. О соотношении понятий «угроза» и «опасность» – [Электронный ресурс] – http://old.nasledie.ru/oboz/N07_97/7_06.HTM (дата обращения 25.03.2020);

35. Цветкова О.Л., Айдинян А.Р. Интеллектуальная система оценки информационной безопасности предприятия от внутренних угроз // Вестник компьютерных и информационных технологий. — 2014. — № 8(122). — С. 48-53. – [Электронный ресурс] – https://cyberleninka.ru/article/n/podhod-k-klasterizatsii-ugroz-informatsionnoy-bezopasnosti-predpriyatiy (дата обращения 20.04.2020);

36. Кучеров И.И. Налоговая тайна в системе мер защиты конфиденциальной информации / Налоговое право России: учебник / отв.ред. Ю.А. Крохина. - 6-е изд., испр. - М.: Норма, 2015. С. 403 – [Электронный ресурс] – https://cyberleninka.ru/article/n/pravovoy-rezhim-zaschity-nalogovoy-informatsii-i-voprosy-ego-optimizatsii (дата обращения 25.04.2020);

37. Айдинян А.Р., Цветкова О.Л., Кикоть И.Р., Казанцев А.В., Каплун В.В. О подходе к оценке информационной безопасности предприятия // Системный анализ, управление и обработка информации: сб. тр. V Междунар. науч. семинара, п. Дивноморское, 2-6 окт. — Ростов н/Д: ДГТУ, 2014. — С.

109-111. – [Электронный ресурс] – http://www.ivdon.ru/uploads/article/pdf/IVD_51_Ajdinyan_Tsvetkova.pdf_da25c0a203.pdf (дата обращения 05.03.2020);

38. Артемов А.В. Информационная безопасность. Курс лекций. Орел: Литагент «МАБИВ», 2014. 51 с. – [Электронный ресурс] – https://royallib.com/book/artemov_a/informatsionnaya_bezopasnost_kurs_lektsiy.html (дата обращения 09.04.2020);

39. Травников Н.О. Конституционно-правовой анализ понятия «право на информацию» // Российский юридический журнал. 2014. N 4. С. 18 - 22. – [Электронный ресурс] – http://www.ruzh.org/?q=node/292 (дата обращения 22.04.2020);

40. Шеховцева Е.В. Налоговая тайна: правовой режим охраны // Ленинградский юридический журнал. 2013. N 1. С. 38 - 42. – [Электронный ресурс] – http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=CJI&n=78577#046840073397521276 (дата обращения 02.05.2020);

41. Средство защиты информации от несанкционированного доступа «Блок-хост—сеть К». Руководство администратора безопасности. СПб., 2013. – [Электронный ресурс] – http://federalbook.ru/files/Reestr/Company/Bezopasnost/NB%201-58-1.pdf (дата обращения 26.03.2020);

42. Ключевые возможности MaxPatrol 8 – [Электронный ресурс] – http://www.ptsecurity.ru/mp8/ (дата обращения: 25.04.2020);

43. ERPScan Security Monitoring Suite – [Электронный ресурс] – http://dsec.ru/products/erpscan/ (дата обращения: 25.04.2020);

44. Шубинский М.И. Информационная безопасность для работников бюджетной сферы. Учебное пособие / НИУ ИТМО. СПб., 2012. – [Электронный ресурс] – https://books.ifmo.ru/file/pdf/934.pdf (дата обращения: 25.04.2020);

45. О расширении процессов модернизации в территориальных налоговых органах МНС России – [Электронный ресурс] – http://base.garant.ru/12129706/#ixzz4ieENUxYv (дата обращения: 25.04.2020);

46. Аронов А.В., Кашин В.А. Налоговая политика и налоговое администрирование: учеб. пособие. М.: Экономист, 2006. 188 с. – [Электронный ресурс] –http://elibrary. ru/item.asp?id=19780724 (дата обращения: 12.04.2020);

47. См.: Михаил Мишустин: «Для людей льготы по налогам на землю и имущество надо сохранить». – [Электронный ресурс] – http://taxpravo.ru/analitika/statya-165158-mihail_mishustin_dlya_lyudey_lgotyi_po_nalogam_na_zemlyu_i_imuschestvo_nado_sohranit_?print=1 (дата обращения: 08.03.2020);

48. Беспалов М.В. Информационное взаимодействие в системе налоговых органов: основные задачи, проблемные точки и перспективы развития // Бухгалтер и закон. 2013. № 5. С. 13—17. – [Электронный ресурс] – http://elibrary.ru/item. asp?id=20500502 (дата обращения: 16.04.2020);

49. Котина Г.А., Карпеева Н.М. Функции налогового администрирования в проекте модернизации ФНС России. Планы и реальность // Актуальные вопросы налогового администрирования: от теории к практике: тез. докл. науч.-практ. конф. Н. Новгород, 21 нояб. 2015 г. Н. Новгород, 2015. С. 26—29. – [Электронный ресурс] – http://elibrary.ru/item.asp?id=25705824 (дата обращения: 20.04.2020);

50. Лиференко А.В. Модернизация автоматизированной информационной системы налогового учета в России // Актуальные проблемы авиации и космонавтики: межвузовский сборник научных трудов. 2016. №12. С. 67-69. – [Электронный ресурс] – https://elibrary.ru/item.asp?id=28146277 (дата обращения: 20.04.2020);

51. АИС «Налог-3» - Новая разработка от ФНС [Электронный ресурс] // Nanalog.ru: [Сайт]. [2013]. – [Электронный ресурс] – http://nanalog.ru/index.php?newsid=887 (дата обращения 16.04.2020);

52. Письмо ФНС России от 13 июля 2017 года № ММВ-20-15/112@ «Об ускоренном возмещении НДС добросовестными налогоплательщиками» – [Электронный ресурс] – http://www.consultant.ru/ (дата обращения 16.04.2020);

53. Александров И.И. Налоги и налогообложение. И.И.Александров. - М.: Крокус, 2017. - 502 с. – [Электронный ресурс] – https://finances.social/nalogooblojenie_828-nalogi/nalogi-nalogooblojenie-uchebnik-aleksandrov.html (дата обращения 16.04.2020);

54. Аронов А.В. Налоги и налогообложение: - М.: Налоги, 2017. - 450 с. – [Электронный ресурс] – https://knigi.news/nalogooblojenie/nalogi-nalogooblojenie-uchebnoe.html (дата обращения 16.04.2020);

55. Архипов А.И. Комментарий к налоговому кодексу РФ - М.: Ланс, 2018. - 600 с. – [Электронный ресурс] – http://www.consultant.ru/document/cons_doc_LAW_19671/ (дата обращения 17.04.2020);

56. Горский И.В. Налоговая политика РФ: проблемы и совершенствование - М.: Финансы, 2016. - 350 с. – [Электронный ресурс] – https://cyberleninka.ru/article/n/aktualnye-problemy-i-puti-sovershenstvovaniya-nalogovoy-sistemy-rossiyskoy-federatsii (дата обращения 17.04.2020);

57. Гарифуллина Г.В. Внедрение АИС «Налог-3» - это реализация инновационных проектов службы / Г.В. Гарифуллина // Материалы первой научно-практической конференции: Изд-во УГАТУ, 2016. С. 72-78. – [Электронный ресурс] – https://cyberleninka.ru/article/n/avtomatizirovannaya-informatsionnaya-sistema-nalog-3-kak-edinoe-tsentralizovannoe-informatsionnoe-prostranstvo-federalnoy-nalogovoy (дата обращения 17.04.2020);

58. Новицкая Е.А., Зубарева Е.Г. Информационные технологии, их развитие в сфере налогообложения и переход налоговых органов на АИС

«НалогЗ» / Е.А. Новицкая, Е.Г. Зубарева // Научный альманах, 2015. № 7. С. 160-163. – [Электронный ресурс] – https://cyberleninka.ru/article/n/avtomatizirovannaya-informatsionnaya-sistema-nalog-3-kak-edinoe-tsentralizovannoe-informatsionnoe-prostranstvo-federalnoy-nalogovoy (дата обращения 17.04.2020);

59. Обязанность Федеральной налоговой службы: материалы Управления информационных технологий ФНС России. – [Электронный ресурс] – https://ppt-online.org/289628/ (дата обращения: 20.04.2020);

60. Еременко С.П., Хитов С.Б. Оценка результативности как важнейший аспект построения системы обеспечения информационной безопасности в системе распределенных ситуационных центров МЧС России // Науч.-аналит. журн. «Вестник С.-Петерб. ун-та ГПС МЧС России». 2016. № 2. С. 84-90. – [Электронный ресурс] – https://cyberleninka.ru/article/n/zaschischennost-slozhnyh-informatsionnyh-sistem-situatsionnyh-tsentrov-mchs-rossii (дата обращения: 20.04.2020);

61. Лапшина С. Н. Информационный менеджмент: методические указания к выполнению лабораторных работ по курсу «Методы управления проектами» – Прикладная информатика [Текст] / сост. С. Н. Лапшина, В. В. Ташлыков. Екатеринбург: УрФУ, 2011. 74 с;

62. Толмачев А.В., Оценка экономической эффективности IT-проектов: методические указания к выполнению ВКР [Текст] / А.В. Толмачев. Екатеринбуг: УрФу, 2020.