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

Факультет математики и информатики
Кафедра информационных и управляющих систем
Направление подготовки 09.03.02 – Информационные системы и технологии
Направленность (профиль) образовательной программы Безопасность информационных систем

ДОПУСТИТЬ К ЗАЩИТЕ
Зав. кафедрой
_____ А.В. Бушманов
«_____»_____ 2022 г.

БАКАЛАВРСКАЯ РАБОТА

на тему: Разработка информационной системы «Управление взаимоотношениями с клиентами» на основе .NET-технологий для ООО «СТОЖАРЫ»

Исполнитель
студент группы 855-об _____ (подпись, дата) Е.Т. Сенашов

Руководитель
доцент, канд. техн. наук _____ (подпись, дата) Т.А. Галаган

Консультант по безопасности и экологичности
доцент, канд. техн. наук _____ (подпись, дата) А.Б. Булгаков

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

Благовещенск 2022

Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
АМУРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
(ФГБОУ ВО «АмГУ»)
Факультет математики и информатики
Кафедра информационных и управляющих систем

УТВЕРЖДАЮ
Зав. кафедрой
_____А.В. Бушманов
«_____» _____ 2022 г.

З А Д А Н И Е

К бакалаврской работе студента Сенашова Е.Т.

1. Тема выпускной квалификационной работы: Разработка информационной системы «Управление взаимоотношениями с клиентами» на основе .NET-технологий для ООО «СТОЖАРЫ»

(утверждена приказом 679-уч от 05.04.2022)

2. Срок сдачи студентом законченной работы: _____

3. Содержание бакалаврской работы (перечень подлежащих разработке вопросов): анализ предметной области и организации, обоснование необходимости разработки и определение требований, проектирование программного продукта, разработка и эксплуатация программного продукта, безопасность и экологичность.

4. Исходные данные к выпускной квалификационной работе: отчет о прохождении преддипломной практики, нормативная документация, специальная литература.

5. Консультанты по выпускной квалификационной работе:
по безопасности и экологичности - Булгаков А.Б., доцент, кандидат технических наук.

6. Дата выдачи задания: 07.02.2022

Руководитель бакалаврской работы: доцент, канд.техн.наук Т.А. Галаган

Задание принял к исполнению(дата): 07.02.2022 Е.Т. Сенашов

РЕФЕРАТ

Выпускная квалификационная работа содержит 76 с., 18 рисунков, 10 таблиц, 2 приложения, 20 источников.

РАЗРАБОТКА, БАЗА ДАННЫХ, АНАЛИЗ, ПРОЕКТИРОВАНИЕ, CRM-СИСТЕМА, ИНФОРМАЦИОННАЯ СИСТЕМА.

В работе реализовано проектирование и разработка информационной системы управления взаимоотношениями с клиентами.

Целью работы является создание ИС, позволяющей упростить основные бизнес-процессы ООО «СТОЖАРЫ», автоматизировать документооборот с клиентами с помощью шаблонов, собирать статистику продаж по сотрудникам и клиентам, производить планирование сделок.

В ходе работы было необходимо:

− проанализировать существующие CRM-системы и деятельность изучаемого общества с ограниченной ответственностью;

− определить цели и функции приложения, выбрать модель жизненного цикла ПО, спроектировать структуру приложения;

− выбрать средства разработки, разработать ИС;

− рассмотреть угрозы ИБ приложения и предложить решения по их устранению.

НОРМАТИВНЫЕ ССЫЛКИ

В настоящей бакалаврской работе использованы ссылки на стандарты и нормативные документы:

ГОСТ Р ИСО/МЭК 27002-2021. Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил применения мер обеспечения информационной безопасности.

ГОСТ 34.601-90. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания.

ГОСТ 30772-2001. Ресурсосбережение. Обращение с отходами. Термины и определения.

ГОСТ Р 51275-2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения.

СП 2.2.3670-20. Санитарно-эпидемиологические требования к условиям труда.

СанПиН 1.2.3685-21. Гигиенические нормативы и требования к обеспечению безопасности и (или) безвредности для человека факторов среды обитания.

СП 52.13330.2016. Естественное и искусственное освещение.

НПБ 105-03. Нормы пожарной безопасности. Определение категорий помещений, зданий и наружных установок по взрывопожарной и пожарной опасности.

Приказ ФСТЭК России от 18 февраля 2013 г. N 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»

Федеральный закон "О персональных данных" от 27.07.2006 N 152-ФЗ

СОКРАЩЕНИЯ, ОБОЗНАЧЕНИЯ И ОПРЕДЕЛЕНИЯ

ЖЦ – жизненный цикл.

ИБ – информационная безопасность.

ИС – информационная система.

ИСПДн – информационная система персональных данных

ООО – общество с ограниченной ответственностью.

ПО – программное обеспечение.

РСП – режимно-секретное подразделение.

СЗИ – средства защиты информации.

ТЗ – техническое задание.

ТЗИ – техническая защита информации.

ФСБ – Федеральная служба безопасности.

ФСТЭК – Федеральная служба транспортного и экспортного контроля.

ЭЦП – электронно-цифровая подпись.

CRM – сокращение от англ. Customer Relationship Management – система управления взаимоотношениями с клиентами.

MVVM – Model – View – ViewModel – архитектурный паттерн.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

В эпоху жестокой конкуренции и фокусировании предприятий на массовые продажи ориентация на уникальность продукта утратила актуальность. Производителей множество, в то время как качество их товаров и оказываемых услуг – приблизительно на одном уровне, так же как и цены. Единственным способом оторваться от конкурентов стало определение и удовлетворение конкретных индивидуальных потребностей клиента.

В силу вышеозначенных обстоятельств одной из наиболее острых проблем, стоящих перед многими предприятиями, является автоматизация. Зачастую бизнес-процесс в организациях достаточно сложен. Но прогресс не стоит на месте и уже существуют десятки способов его упростить.

Система управления взаимоотношениями с клиентами – это один из наиболее комплексных и универсальных вариантов решения этой проблемы. Универсальность такой системы достигается за счёт количества функций, которые могут в ней присутствовать. Верным будет утверждение, что такая система – это программа-конструктор, состоящий из множества небольших модулей, каждый из которых в той или иной степени упрощает работу.

По данным корпорации Zendesk более 90% зарубежных компаний с численностью сотрудников больше 11 человек используют системы управления взаимоотношениями с клиентами. В России этот показатель значительно ниже, в том числе и по причине малого количества доступных продуктов полностью на русском языке и с русскоязычной поддержкой.

Целью работы является создание упрощённой системы управления взаимоотношения с клиентами, которая будет содержать только минимально необходимый набор функций с возможностью последующей модификации и добавления: сбор статистики продаж и представление её различными способами, автоматизация документооборота путём быстрого использования шаблонов, управление продажами через отслеживание предыдущих и текущих взаимодействий с клиентом.

1 АНАЛИЗ CRM-СИСТЕМ

1.1 Классификация CRM-систем

Система управления взаимоотношениями с клиентами (CRM-система) – прикладное программное обеспечение, создаваемое для автоматизации взаимодействий с заказчиками, в том числе для увеличения продаж, и улучшения качества обслуживания клиентов с помощью сбора и хранения информации о клиентах, улучшения бизнес-процессов и последующего анализа результатов.

CRM — модель взаимодействия, в которой центром всего бизнеса является клиент, а главными направлениями деятельности компании являются меры по обеспечению эффективных продаж и качественного обслуживания клиентов. Поддержка этих целей включает сбор, хранение и анализ информации о клиентах, поставщиках и партнёрах.

По версии Пола Гринберга существует всего 2 основных классификации систем управления взаимоотношениями с клиентами.

По назначению:

- автоматизированная система управления продажами;
- управление маркетингом;
- системы по обработке обращений абонентов.

Классификация по уровню обработки информации:

- операционный CRM – регистрация и оперативный доступ к первичной информации по событиям, компаниям, проектам, контактам;
- аналитический CRM – отчётность и анализ информации;
- коллаборативный CRM – опросы, для изменения качеств продукта или порядка обслуживания, веб-страницы для отслеживания клиентами состояния заказа, уведомления о событиях, связанных с заказом, возможность для клиента самостоятельно выбрать и заказать в режиме реального времени продукты и услуги.

1.2 Сравнительный анализ существующих решений

В настоящий момент существует относительно небольшое количество решений, полностью подходящих функционально условиям работы предприятий малого и среднего бизнеса. Ещё меньше из них – на русском языке, и буквально единицы имеют русскоязычную поддержку. Надо ли говорить о том, что каждый оставшийся условно-подходящий вариант имеет свои недостатки и сложности в работе с ним. Это может быть неподъёмный ценник, высокие системные требования, неудобство в использовании за счёт недружелюбного интерфейса и многое другое.

По причине того, что в ООО «СТОЖАРЫ» не используется в данный момент какая-либо CRM-система, рассмотрим готовые сторонние решения. Для дальнейшего рассмотрения выбраны такие CRM-системы как Zoho CRM, 1С CRM и Битрикс24. Упоминания достойны также такие системы как AmoCRM, Prostoy CRM и система от NetHunt.

Zoho CRM является разработкой Zoho Corporation, расположенной в Индии. Именно поэтому у неё отсутствует техническая поддержка на русском языке. Кроме того, цены на данный программный продукт представлены в долларах, и стоит эта система 600 долларов в год за 1 рабочее место. Это по российским меркам считается неподъёмной ценой для предприятий малого и среднего бизнеса. Стоит, однако, отметить, что некоторые крупные компании всё же используют данную систему, несмотря на расценки.

Данная система очень популярна за рубежом, но в первую очередь среди предприятий среднего и крупного бизнеса в англоговорящих странах. Возможность использования системы на национальном языке страны имеется у весьма скромного списка государств. Россия в это число входит, но перевод является машинным. Это приводит к тому, что немногочисленные пользователи данной CRM-системы из России вынуждены пользоваться ей на английском.

Пример её интерфейса представлен на рисунке 1.

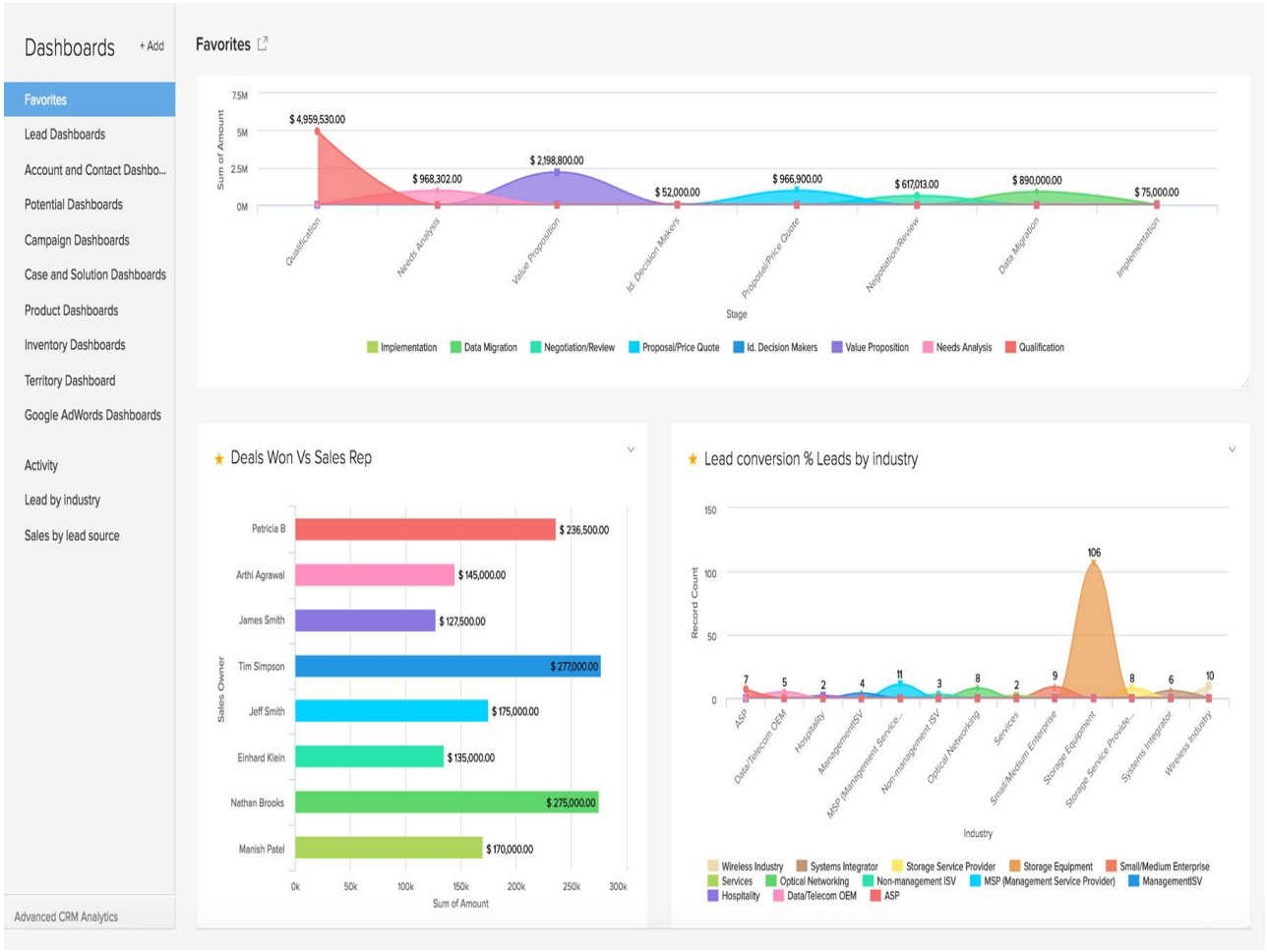

Рисунок 1 – Вид интерфейса Zoho CRM

1С CRM – система от компании 1С. Лицензия на 1 месяц на 1 рабочее место стоит 14500 рублей. Она полностью совместима с другими продуктами от фирмы 1С, но это же накладывает и определённые трудности. Данная CRM-система очень плохо интегрируется с базами данных, управляемыми СУБД не от 1С.

При кажущейся простоте интерфейса он абсолютно недружелюбен к пользователю. Поэтому перед началом использования данной системы фирма 1С рекомендует пройти курс по обучению работе с ней всем потенциальным пользователям. Пример её интерфейса представлен на рисунке 2.

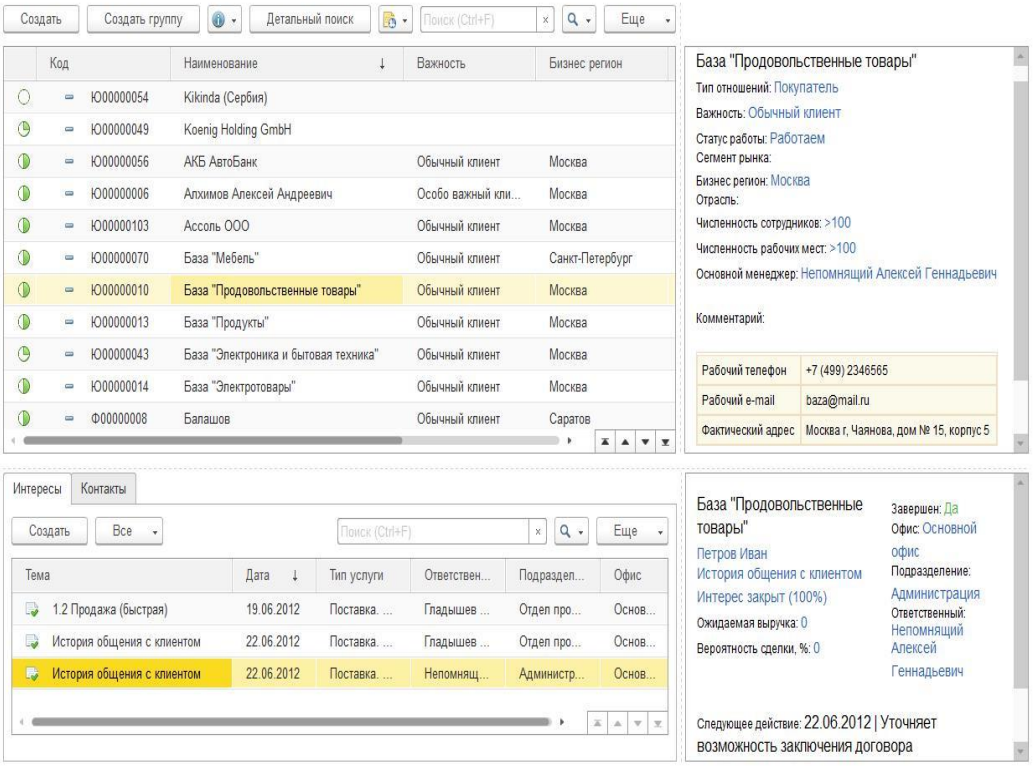

Рисунок 2 – Вид интерфейса 1С CRM

Битрикс24 – CRM-система от компании 1С-Битрикс, дочерней компании 1С. Пример интерфейса Битрикс24 представлен на рисунке 3.

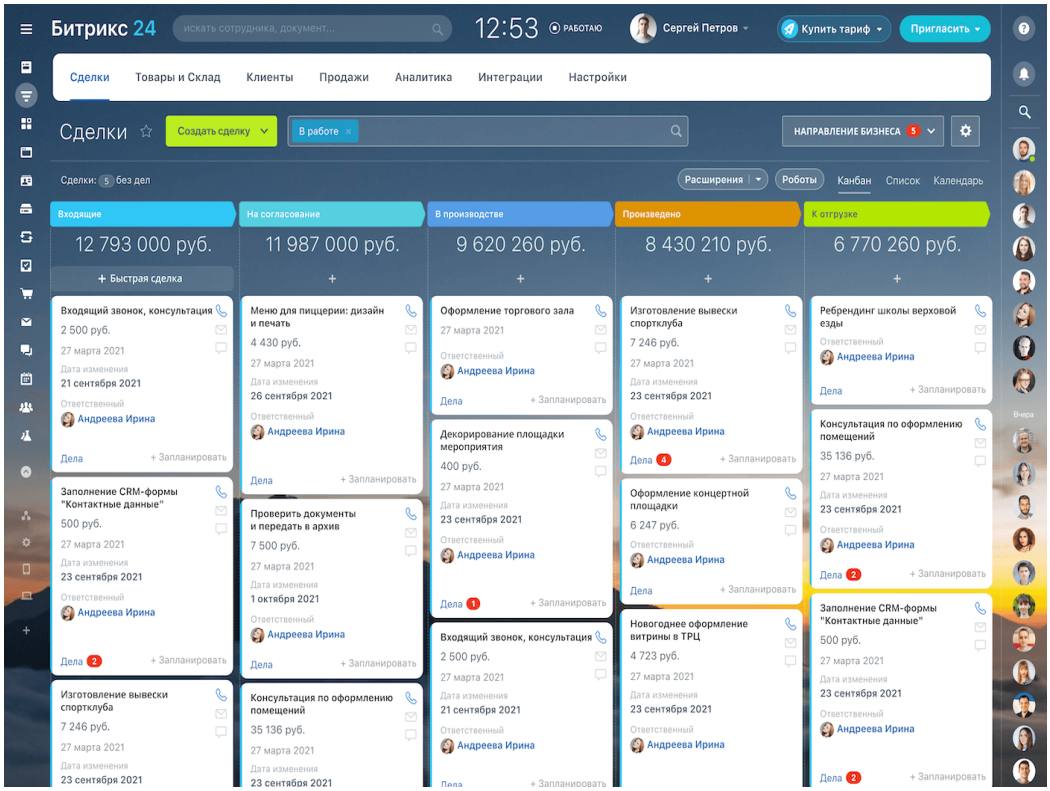

Рисунок 3 – Вид интерфейса Битрикс24

1С-Битрикс известна как разработчик одной из самых популярных CMS в СНГ. Этим объясняется тот факт, что Битрикс24 основана на web-технологиях. У данной системы существует бесплатная версия, платная годовая лицензия на 5 пользователей стоит от 60000 рублей в год.

При целом комплексе достоинств данной CRM-системы, таких как гибкость настройки, дружелюбность интерфейса, сравнительно низкая цена, полная поддержка русского языка и прочих, есть один крайне существенный недостаток – безопасность.

В силу того, что в Битрикс24 используются web-технологии, а сама она основана на прежних разработках 1С-Битрикс, данные хранятся по принципу хостинга сайтов или иных web-сервисов – на выделенных серверах компании или в облачных хранилищах. Таким образом, чтобы пользоваться данной системой управления взаимоотношениями с клиентами, необходимо передавать используемые данные на сервера компании через Интернет. Понятно, что в таком случае невозможно использовать данную CRM-систему в ИСПДн или тем более защищённых ГИС по требованиям безопасности. Кроме того страдает автономность, например при использовании Битрикс24 в локальных сетях без подключения к сети Интернет.

2 АНАЛИЗ ДЕЯТЕЛЬНОСТИ ООО «СТОЖАРЫ»

2.1 Общее положение

Предметом деятельности Общества являются:

- производство, проведение испытаний, закупка и поставка пожарно-технической продукции;
- обучение населения мерам пожарной безопасности;
- осуществление противопожарной пропаганды, издание специальной литературы и рекламной продукции;
- монтаж, техническое обслуживание и ремонт систем и средств противопожарной защиты;
- ремонт и обслуживание пожарного снаряжения первичных средств тушения пожаров, восстановление качества огнетушащих средств;
- внешнеэкономическая деятельность:
- создание совместных предприятий с иностранными юридическими и физическими лицами;
- осуществление экспортно-импортных операций, в том числе экспортирование произведенной обществом продукции (работ, услуг);
- осуществление деятельности по сбору, хранению, утилизации, переработке и реализации лома и отходов черных металлов, и экспорту лома и отходов черных металлов;
- проектирование, монтаж, пуско-наладка. техническое облуживание, ремонт систем охранно-пожарной, тревожной сигнализации, видеонаблюдения, контроля доступа и оповещения о пожаре;
- огнезащита конструкции;
- работы по устройству внутренних инженерных систем и оборудования;
- монтаж, пуско-наладка, ремонт и техническое обслуживание систем и средств противопожарной защиты;

– осуществление строительно-монтажных работ на объектах военной инфраструктуры;

– проведение контроля защищенности информации ограниченного доступа;

– аттестационные испытания и аттестация объектов информатизации на соответствие требованиям по защите информации;

– проведение спец. исследований на побочные электромагнитные излучения и наводки;

– проектирование объектов в защищенном исполнении;

– реализация, установка, монтаж, наладка, испытание, ремонт и сервисное обслуживание средств защиты информации;

– осуществление работ, связанных с использованием сведений, составляющих государственную тайну;

– оказание услуг в области защиты государственной тайны;

– предоставление услуг по монтажу, ремонту и техническому обслуживанию приборов и инструментов для измерения, контроля, испытания, навигации, локации и прочих целей;

– производство общестроительных работ по прокладке местных трубопроводов, линий связи и линий электропередачи, включая взаимосвязанные вспомогательные работы;

– розничная торговля оборудованием электросвязи;

– консультирование по аппаратным средствам вычислительной техники;

– разработка программного обеспечения и консультирование в этой области;

– техническое обслуживание и ремонт офисных машин и вычислительной техники;

– разработка защищенных с использованием шифровальных (криптографических) средств информационных систем;

– разработка защищенных с использованием шифровальных (криптографических) средств телекоммуникационных систем;

– производство (тиражирование) шифровальных (криптографических) средств;

– производство защищенных с использованием шифровальных (криптографических) средств информационных систем;

– производство защищенных с использованием шифровальных (криптографических) средств телекоммуникационных систем;

– производство средств изготовления ключевых документов;

– изготовление с использованием шифровальных (криптографических) средств изделий, предназначенных для подтверждения прав (полномочий) доступа к информации и (или) оборудованию в информационных и телекоммуникационных системах;

– монтаж, установка (инсталляция), наладка шифровальных (криптографических) средств;

– монтаж, установка (инсталляция), наладка защищенных с использованием шифровальных (криптографических) средств информационных систем;

– монтаж, установка (инсталляция), наладка защищенных с использованием шифровальных (криптографических) средств телекоммуникационных систем;

– монтаж, установка (инсталляция), наладка средств изготовления ключевых документов;

– работы по обслуживанию шифровальных (криптографических) средств, предусмотренные технической и эксплуатационной документацией на эти средства;

– предоставление услуг по шифрованию информации, не содержащей сведений составляющих государственную тайну, с использованием шифровальных (криптографических) средств в интересах юридических и физических лиц, а также индивидуальных предпринимателей;

− предоставление услуг по защите информации, не содержащей сведений, составляющих государственную тайну. с использованием шифровальных (криптографических) средств в интересах юридических и физических лиц, а также индивидуальных предпринимателей:

− предоставление юридическим и физическим лицам защищенных с использованием шифровальных (криптографических) средств каналов связи для передачи информации;

− изготовление и распределение ключевых документов и (или) исходной ключевой информации для выработки ключевых документов с использованием аппаратных, программных и программно-аппаратных средств, систем и комплексов изготовления и распределения ключевых документов для шифровальных (криптографических) средств;

− передача шифровальных (криптографических) средств;

− передача защищенных с использованием шифровальных (криптографических) средств информационных систем;

− передача защищенных с использованием шифровальных (криптографических) средств телекоммуникационных систем;

− передача средств изготовления ключевых документов;

− производство цифровых вычислительных машин, аналоговых вычислительных машин, гибридных вычислительных машин, периферийных устройств (принтеров, терминалов и т.п.), магнитных и оптических считывающих устройств, машин для записи данных в кодированной форме на носители данных и др.;

− установку компьютеров и прочего оборудования для обработки информации (предоставление услуг);

− деятельность в области телематических служб: факсимильной службы, службы обработки сообщении и электронной почты, службы телеконференций, информационной службы, включая справочные службы и службы доступа к информационным ресурсам, службы голосовой связи, службы передачи речевой информации с использованием пакетной коммуникации;

− деятельность в области передачи данных и обмену информацией между персональными компьютерами, предоставление доступа к глобальным компьютерным сетям и места для размещения информации в них;

− осуществление иной деятельности, которая прямо, или косвенно способствует осуществлению стоящих перед обществом задач;

− иные виды деятельности, не противоречащие действующему законодательству.

Место нахождение общества с ограниченной ответственностью «СТО-ЖАРЫ»: Амурская область, город Благовещенск, ул. Батарейная, 26/4.

Общество имеет право:

− в порядке, установленном законом, участвовать в деятельности и создавать в российской федерации и других странах хозяйственные общества и другие предприятия и организации с правами юридического лица;

− участвовать в ассоциациях и объединениях других видов;

− участвовать в деятельности и сотрудничать в любой иной форме с международными общественными, кооперативными и иными организациями;

− приобретать и реализовывать продукцию (работы, услуги) других обществ, предприятий, объединений и организации, а также иностранных фирм как в российской федерации, так и за рубежом в соответствии с действующим законодательством;

− осуществлять иные права и нести другие обязанности в соответствии с действующим законодательством.

Общество вправе привлекать для работы российских и иностранных специалистов, самостоятельно определяя формы, размеры и виды оплаты труда.

Общество в целях реализации технической, социальной, экономической и налоговой политики несет ответственность за сохранность документов (управленческих, финансово-хозяйственных, по личному составу и др.); обеспечивает передачу на государственное хранение документов, имеющих научно-историческое значение, в государственные архивные учреждения в соответ-

ствии с действующим законодательством; хранит и использует в установленном порядке документы по личному составу.

Для достижения целей своей деятельности Общество может приобретать права, принимать обязанности и осуществлять любые действия, не запрещенные законодательством. Деятельность Общества не ограничивается оговоренной в Уставе. Сделки, выходящие за пределы уставной деятельности, но не противоречащие закону, являются действительными.

2.2 Организационная структура ООО «СТОЖАРЫ»

ООО "СТОЖАРЫ" специализируется на обеспечении организаций различных форм собственности пожарно-спасательным инвентарем и оборудованием, установке и обслуживании охранно-пожарной сигнализации, систем видеонаблюдения и контроля доступа, систем оповещения, изготовлении специальных информационных знаков и планов эвакуации, выполнении работ по огнезащитной обработке объектов, обслуживанию огнетушителей, а также на оказании услуг в области информационной безопасности: проведение аттестаций, обеспечение организаций средствами защиты информации, администрирование и техническая поддержка.

Структура ООО "СТОЖАРЫ", приведенная в таблице 1, утверждена генеральным директором.

Таблица 1 – Структура предприятия ООО «СТОЖАРЫ»

Структурное подразделение	Должность (специальность, профессия)	Количество штатных единиц
1	2	3
Дирекция	Генеральный директор	1
	Директор	1
	Специалист по кадрам	1
Бухгалтерия	Главный бухгалтер	1
	Бухгалтер	2
Инженерно-технический отдел	Начальник	1
	Инженер	1
	Техник по обслуживанию ОПС	2
	Техник-сметчик	1

Продолжение таблицы 1

1		2	3
Отдел продаж		Начальник	1
		Менеджер по работе с клиентами	1
		Менеджер	2
		Заведующий складом	1
Цех по облуживанию и ремонту средств пожаротушения		Ведущий специалист по техническому обслуживанию и ремонту огнетушителей	1
		Специалист по техническому обслуживанию и ремонту огнетушителей	2
Отдел транспортной безопасности		Начальник	1
		Специалист по физической подготовке	1
		Психолог	1
Управление информационной безопасности	Начальник		1
	Отдел технической поддержки	Начальник отдела технической поддержки	1
		Ведущий специалист технической поддержки	1
		Специалист отдела технической поддержки	2
	Торговый отдел	Начальник торгового отдела	1
		Ведущий специалист торгового отдела	1
		Специалист торгового отдела	1
		Менеджер торгового отдела	1
Отдел технической защиты информации		Начальник	1
		Ведущий специалист	2
		Специалист	1
Гараж		Водитель	1
Режимно-секретное подразделение		Начальник	1
		Делопроизводитель	1

На основе таблицы 1 составим схему организационной структуры ООО «СТОЖАРЫ», представленную на рисунке 4.

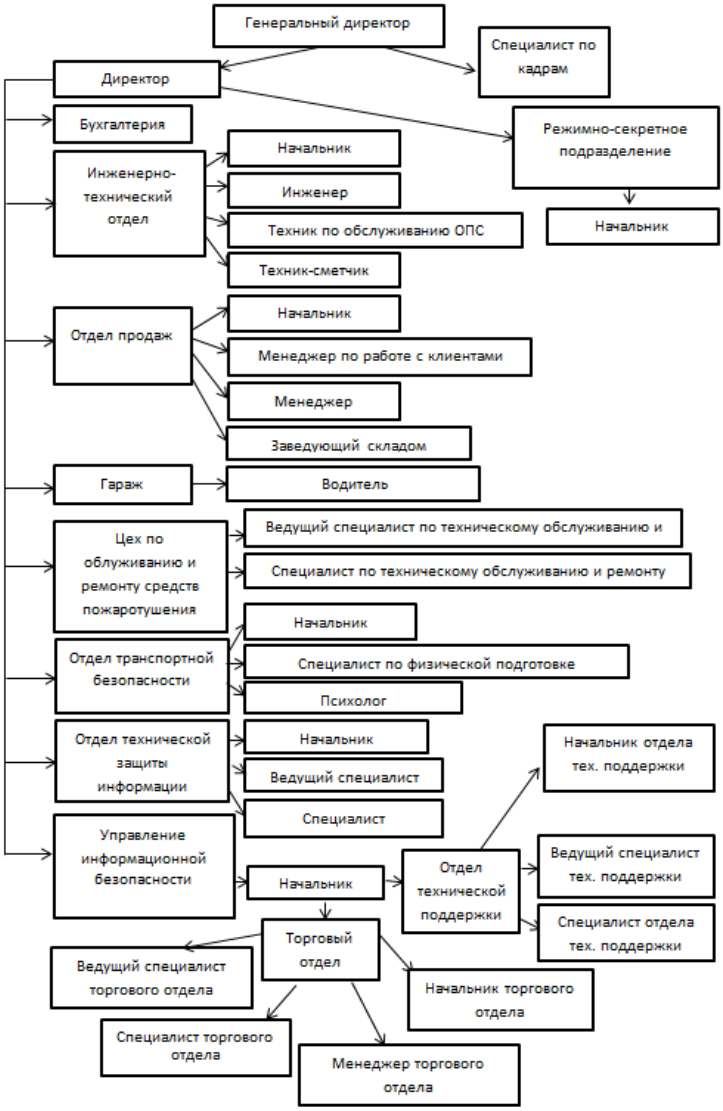

Рисунок 4 – Организационная структура ООО «СТОЖАРЫ»

В организационную структуру Общества с ограниченной ответственностью «СТОЖАРЫ» входят:

– отдел продаж занимается продажей различного противопожарного оборудования: огнетушители, пожарные шкафы, щиты, рукава, головки;

– цех по облуживанию и ремонту средств пожаротушения занимается заправкой, техническим обслуживанием и ремонтом огнетушителей;

– отдел технической защиты информации занимается проектами по защите информации от утечки по техническим каналам на объектах информатизации, основанные на трех основных составляющих: организационно-распорядительные мероприятия; пассивные меры защиты; активные меры защиты;

– управление информационной безопасности занимается поставками различного программного обеспечения, операционных систем, выпуском ЭЦП, аттестацией объектов ИСПДн, продажей, настройкой и сопровождением СЗИ;

– дирекция занимается управлением ООО «СТОЖАРЫ»;

– бухгалтерия предназначена для сбора данных об имуществе и обязательствах предприятия;

– инженерно-технический отдел занимается техническим обслуживанием турникетов, составлением планов эвакуации, системами видеонаблюдения, пожарно-охранной сигнализацией, системами пожаротушения;

– отдел транспортной безопасности занимается аттестацией людей обеспечивающих транспортную безопасность;

– режимно-секретное подразделение занимается деятельностью, связанной с обработкой секретной информации.

2.3 Состав аппаратного и программного обеспечения

В управлении информационной безопасности есть семь компьютеров, разделенных на два отдела. Три компьютера отдела продаж ИБ и четыре компьютера отдела технической поддержки. Все компьютеры имеют следующие характеристики:

– процессор Intel Core i5-9400F 2.9GHz;

– материнская плата ASUS Prime B365M-A;

– оперативная память 4Gb DDR4 Kingston;

– видео карта Intel UHD Graphics 610;

– SSD накопитель Kingston A2000 250Gb M.2;

– жесткий диск Seagate Barracuda 1Tb SATA-III.

На всех компьютерах установлено следующее программное обеспечение: ОС Windows 10, Microsoft Office 2016, ViPNet CSP, CryptoPro, Visio, Google Chrome, Kaspersky Endpoint Security. Также в управлении информационной безопасности есть сетевой принтер данной модели–HP LaserJet Pro MFP M227sdn.

В торговом отделе в распоряжении есть три компьютера со следующими характеристиками:

– процессор Intel Pentium G6400 4.0GHz;
– материнская плата GIGABYTE H410M;
– оперативная память 4Gb DDR4 Kingston;
– видео карта Intel UHD Graphics 610;
– жесткий диск Seagate Barracuda 1Tb SATA-III.

На всех компьютерах установлено следующее программное обеспечение: ОС Windows 10, Microsoft Office 2013, Google Chrome, Kaspersky Endpoint Security.

В торговом отделе стоит сетевой принтер – KYOCERA ECOSYS M2235dn.

В бухгалтерии стоят два компьютера, их характеристики представлены ниже:

– процессор Intel Core i3-9100 3.6GHz;
– материнская плата ASUS PRIME B365-K;
– оперативная память 4Gb DDR4 Kingston;
– видео карта Intel UHD Graphics 630;
– жесткий диск Seagate Barracuda 1Tb SATA-III.

На всех компьютерах установлено следующее программное обеспечение: ОС Windows 10, Microsoft Office 2013, Google Chrome, 1С:Бухглатерия, 1С:Предприятие, Kaspersky Endpoint Security. В бухгалтерии стоит сетевой принтер–KYOCERA ECOSYS M2235dn.

Компьютер директора обладает следующими характеристиками:

– процессор Intel Core i3-9100 3.6GHz;
– материнская плата ASUS PRIME B365-K;
– оперативная память 4Gb DDR4 Kingston;
– видео карта Intel UHD Graphics 630;
– жесткий диск: Seagate Barracuda 1Tb SATA-III;
– SSD накопитель Kingston A2000 250Gb M.2.

На компьютере установлено следующее программное обеспечение: ОС Windows 10, Microsoft Office 2016, Google Chrome, Kaspersky Endpoint Security. В кабинете директора стоит принтер–HP LaserJet 107w.

Компьютер отдела транспортной безопасности обладает следующими характеристиками:

- процессор Intel Pentium G6400 4.0GHz;
- материнская плата GIGABYTE H410M;
- оперативная память 4Gb DDR4 Kingston;
- видео карта Intel UHD Graphics 610;
- жесткий диск Seagate Barracuda 1Tb SATA-III.

На компьютере установлено следующее программное обеспечение: ОС Windows 10, Microsoft Office 2016, Google Chrome, Dallas Lock, ViPNet Client, Kaspersky Endpoint Security. В отделе транспортной безопасности стоит принтер – HP LaserJet Pro MFP M227sdn.

В инженерно-техническом отделе стоят два компьютера со следующими характеристиками:

- процессор Intel Core i3-10100 3.6GHz;
- материнская плата GIGABYTE H410M S2H;
- оперативная память 4Gb DDR4 Kingston;
- видео карта Intel UHD Graphics 630;
- SSD накопитель GIGABYTE GP-GSTFS 256Gb SATA-III;
- жесткий диск Seagate Barracuda 1Tb SATA-III.

На всех компьютерах установлено следующее программное обеспечение: ОС Windows 10, Microsoft Office 2016, Google Chrome, Visio, Kaspersky Endpoint Security. В инженерно-техническом отделе стоит принтер–Xerox Phaser 3020.

Компьютер генерального директора и специалиста по кадрам имеют следующие характеристики:

- процессор Intel Pentium G5420 3.8GHz;

– материнская плата ASUS PRIME H310M-R;
– оперативная память 4Gb DDR4 Kingston;
– видео карта Intel UHD Graphics 610;
– SSD накопитель GIGABYTE GP-GSTFS 120Gb SATA-III;
– жесткий диск Seagate Barracuda 1Tb SATA-III.

На всех компьютерах установлено следующее программное обеспечение: ОС Windows 10, Microsoft Office 2013, Google Chrome, Kaspersky Endpoint Security. В кабинете генерального директора и специалиста по кадрам стоит принтер – HP LaserJet Pro M404dw.

В отделе технической защиты информации стоят четыре компьютера, характеристики приведены ниже:

– процессор: Intel Core i3-9100 3.6GHz;
– материнская плата: ASUS PRIME B365-K;
– оперативная память: 4Gb DDR4 Kingston;
– видео карта: Intel UHD Graphics 630;
– жесткий диск: Seagate Barracuda 1Tb SATA-III.

На всех компьютерах установлено следующее программное обеспечение: ОС Windows 10, Microsoft Office 2016, Google Chrome, Kaspersky Endpoint Security. В отделе технической защиты информации стоит сетевой принтер – KYOCERA ECOSYS M2235dn.

Локальная сеть в ООО «СТОЖАРЫ» построена по топологии звезда, по стандарту 100Base-T. В неё входит 2 сервера, основной, используемый в качестве хранилища, и дополнительный прокси-сервер. На границе с сетью Интернет расположен аппаратный межсетевой экран. Для обеспечения разграничения доступа использованы 3 маршрутизатора. Схема сети предприятия представлена на рисунке 5.

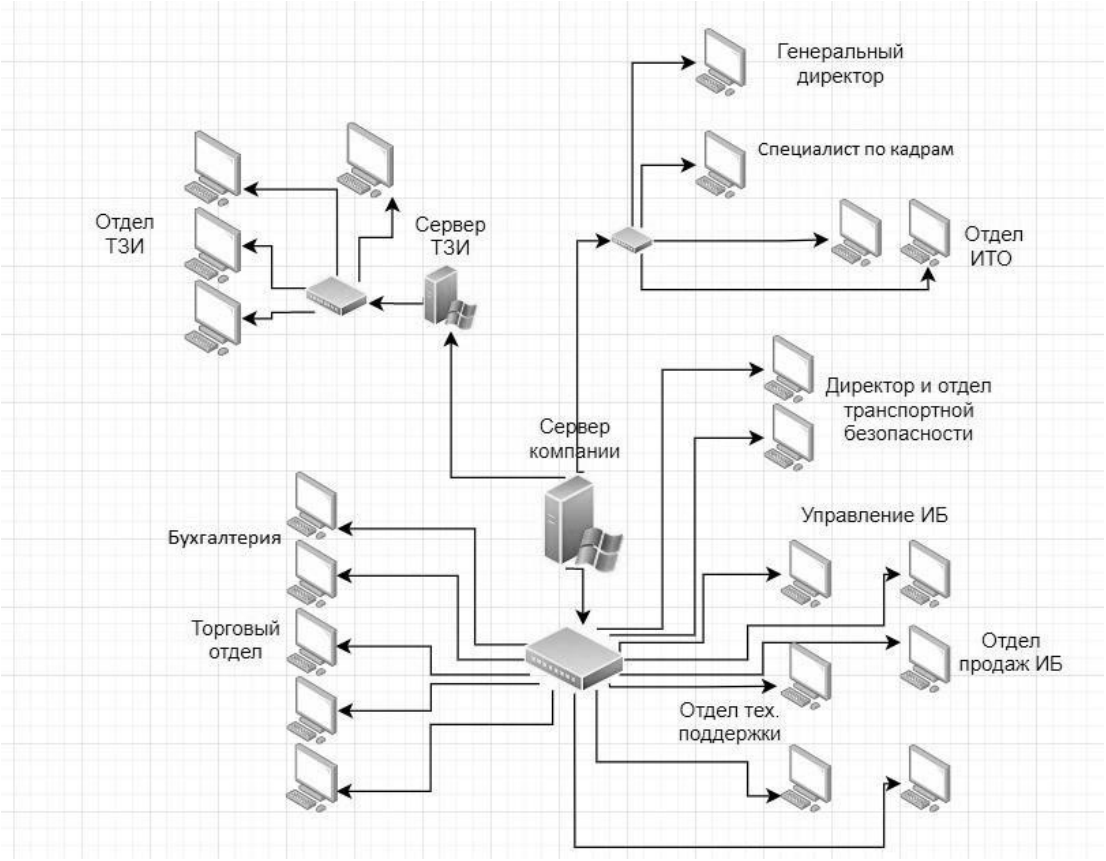

Рисунок 5 – Схема сети ООО «СТОЖАРЫ»

Главный сервер компании используются в качестве интернет-сервера откуда интернет раздается на все остальные рабочие станции. Также у отдела технической защиты информации есть свой сервер и своя подсеть.

2.4 Анализ документооборота

Документооборот – ряд правил, по которым осуществляется перемещение документов в организации. Документы включают в себя цепочку важных процессов учреждения, поэтому в большинстве случаев требуется подпись вышестоящего руководства.

2.4.1 Анализ внешнего документооборота

Внешний документооборот – это все входящие и исходящие документы компании, которыми она обменивается с контрагентами, клиентами и контролирующими органами. К ним относятся коммерческие предложения, счета-фактуры, накладные, акты выполненных работ, договора и другие виды документов. Внешний документооборот ООО «СТОЖАРЫ» представлен на рисунке 6.

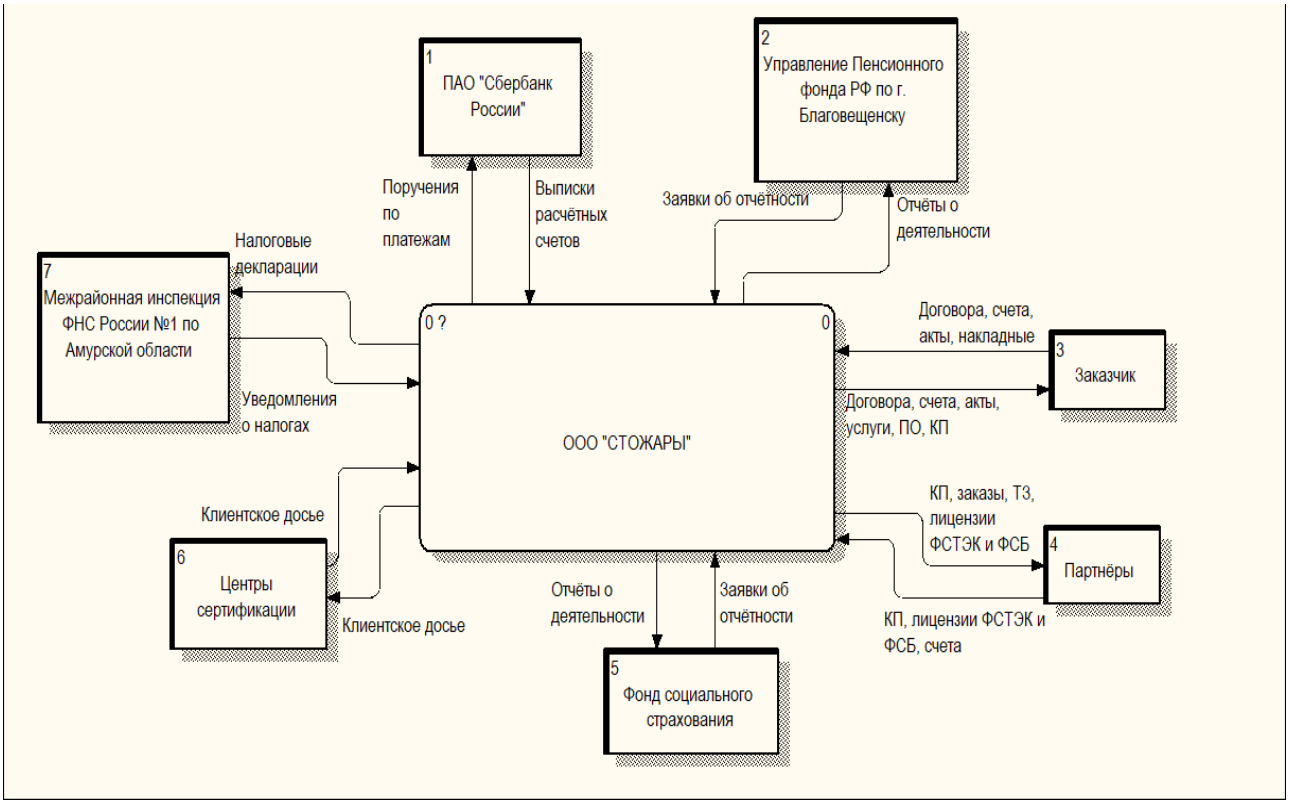

Рисунок 6 – Внешний документооборот ООО «Стожары»

Заказчик запрашивает у компании договора, счета, акты и накладные, на что получает договора, счета, акты, услуги, ПО.

Компания заказывает у партнеров ТЗ, лицензии ФСТЭК и ФСБ и получает ответ в виде сертификатов, лицензий и счетов.

Фонд социального страхования подает заявки об отчетности, а компания отсылает отчеты о деятельности.

Центры сертификации обмениваются с компанией клиентскими досье.

Управление пенсионного фонда подает заявки об отчетности, а компания отсылает отчеты о деятельности.

Компания отправляет Сбербанку поручения по платежам, а банк отвечает выписками расчетных счетов.

Межрайонная налоговая инспекция уведомляет о налогах компанию, на что та отвечает налоговыми декларациями.

Поскольку в ООО «СТОЖАРЫ» нет собственной базы данных, а документооборот производится в ручном режиме (рукописные журналы договоров

и прочих документов), было принято решение автоматизировать самую трудоёмкую его часть – документооборот с заказчиками.

2.4.2 Анализ внутреннего документооборота

Внутренний документооборот позволяет транспортировать документы и новости между структурными подразделениями и всеми сотрудниками компании. К внутреннему документообороту относятся приказы, устав, заявления, протоколы совещаний, инструкции, положения о структурных подразделениях, служебные записки и другие документы. Внутренний документооборот ООО «СТОЖАРЫ» представлен на рисунке 7.

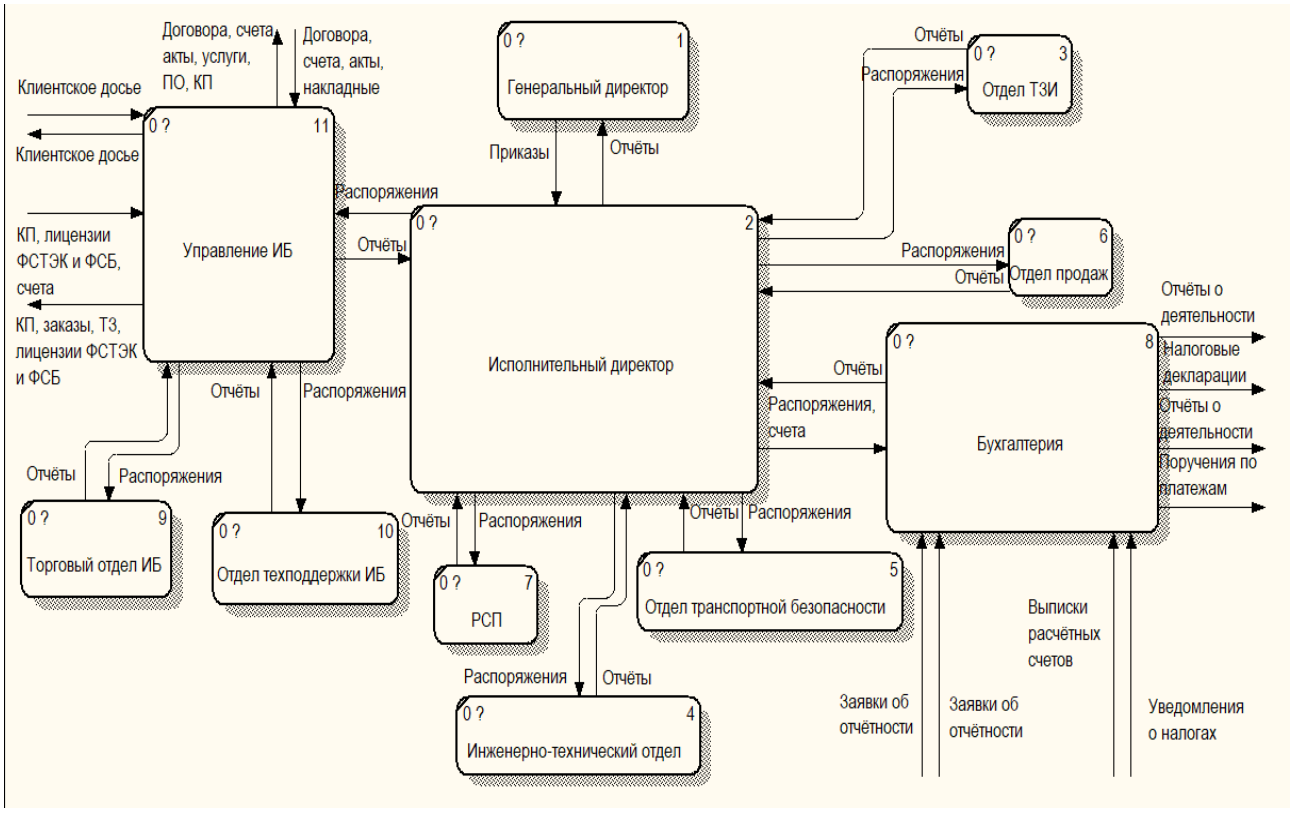

Рисунок 7 – Внутренний документооборот ООО «Стожары»

Генеральный директор отдает приказы исполнительному директору, в ответ на которые ждет отчеты.

Исполнительный директор отдает распоряжения:

- бухгалтерии;
- отделу ТЗИ;
- инженерно-техническому отделу;
- отделу транспортной безопасности;

- отделу продаж;
- РСП;
- управлению ИБ.

Отделы отвечают на распоряжения исполнительного директора отчётами.

Управление ИБ отдает распоряжения торговому отделу ИБ, и в ответ получает отчеты.

Управление ИБ отдает распоряжения отделу технической поддержки ИБ, и в ответ получает отчеты.

3 ПРОЕКТИРОВАНИЕ ИНФОРМАЦИОННОЙ СИСТЕМЫ УПРАВЛЕНИЯ ВЗАИМООТНОШЕНИЯМИ С КЛИЕНТАМИ

3.1 Назначение и цели создания системы

Проектируемая система должна быть ориентирована на решение следующих задач:

– автоматизация документооборота ООО «СТОЖАРЫ» по работе с клиентами;

– создание договоров, коммерческих предложений, спецификаций и актов приёма-передачи прав по шаблонам;

– отслеживание статистики по клиентам (какие продукты, кому и в каких количествах продавались в последний месяц/квартал/год);

– сбор данных о клиентах (ФИО, номер телефона, электронная почта, наименование организации);

– расчёт эффективности направлений работы и отдельных сотрудников по количеству проведённых сделок;

– хранение и визуализация данных для удобной работы с ними оператора ИС.

Целью создания системы является упрощение основных бизнес-процессов, повышение эффективности работы ООО «СТОЖАРЫ», снижение временных затрат на составление документов и сбор данных.

3.2 Разработка проекта автоматизации

3.2.1 Выбор модели жизненного цикла ПО

Жизненный цикл (ЖЦ) ИС – это период разработки и эксплуатации ИС, который начинается с момента возникновения потребности в ИС и заканчивается на этапе её вывода из эксплуатации.

Отношения между системой и ее системными элементами обычно рассматривается как иерархия до простейших ее составляющих. Для сложных систем, системные элементы на каждом отдельном этапе можно рассматривать как систему, чтобы упростить процесс разработки. Таким же способом рекур-

сивно применяются к рассматриваемой системе и соответствующие процессы жизненного цикла системы, хоть и не всегда система подразумевает иерархические отношения, например, как в сетях или иных распределенных системах.

Под моделью ЖЦ понимается структура, которая определяет взаимосвязи задач, действий и процессов на протяжении всего ЖЦ. Основными моделями ЖЦ, которые используются в настоящее время, являются: каскадная, инкрементная и спиральная.

Каскадная и инкрементная модели ЖЦ совпадают и включают в себя следующие этапы:

- анализ требований;
- проектирование;
- программирование;
- тестирование и отладка;
- ввод в действие, эксплуатация и сопровождение.

Каскадная модель подразумевает разработку ПО, когда все этапы разработки происходят последовательно, при этом, каждый последующий шаг начинается только после полного завершения выполнения предыдущего шага. Результатам каждого шага является промежуточный продукт, который не может изменяться на последующих шагах. Данная модель удобна для разработки с чёткими и неизменяемыми в течении ЖЦ требованиям. Также, данная модель пригодна при разработке продукта подразумевающего выпуск новой версии этого продукта или для ПО такого типа, которые разрабатывались разработчиками ранее.

Инкрементная модель похожа на каскадную, но в данном случае, разработка ведётся в несколько инкрементов (версий), которые подразумевают улучшение продукта, пока ЖЦ разработки ПО не прекратится. Это означает, что на каждом этапе ЖЦ возможны обратные связи, которые являются межэтапными корректировками. При этом, процесс ЖЦ растягивается на весь период разработки. Работа над проектом начинается с определения основных требований к системе. Далее, разработчик по принципу приращений, добавляет

определенную функциональность в систему, при этом сначала разрабатывает компоненты с наивысшим приоритетом и постепенно их детализирует. В то же время, возможны уточнение требований других частей системы. При разработке определенно работающего компонента, он предоставляется клиенту, который может уточнить требования на основе использования этого компонента.

Недостатки и достоинства у этой модели такие же, как и у каскадной, но при этом заказчик раньше увидит результат и сможет скорректировать требования. Причём корректировка требований не станет настолько же затратной процедурой как в каскадной модели. Основным недостатком является ухудшение структуры системы, когда при добавлении новых компонентов и изменение требований ухудшают структуру системы. Чтобы избежать этого, нужно дополнительное время на рефакторинг.

При ЖЦ *спиральной модели* на каждом витке спирали выполняется создание очередной версии продукта. На каждой версии происходит уточнение требований проекта и планируются работы следующего витка, если необходимое качество продукта ещё не достигнуто. Анализу и проектированию уделяются особое внимание на начальных этапах разработки, так как это позволяет легче проверять технические решения и реализуемость конкретного проекта и таким образом можно обосновать создание следующего прототипа. Данная модель позволяет уделять внимание рискам, влияющим на организацию жизненного цикла, что является недостатком для проектов, имеющих низкую степень риска, так как оценка рисков на каждом витке ведёт к большим затратам. Модель сочетает в себе возможности модели прототипирования и каскадной модели. Главная же задача, как можно быстрее предоставить заказчику работоспособный продукт.

Целью дипломного проекта является разработка информационной системы управления взаимодействиями с клиентами. Так как на этапе кодирования возможны определенные изменения и, при этом, необходимо предъявлять заказчику каждый модуль и согласовывать с ним необходимые изменения, например для интерфейса и функционала приложения как для администратора,

так и для пользователя, было принято решение использовать инкрементную модель ЖЦ.

На этапе анализа необходимо собрать информацию о том, какие именно этапы бизнес-процесса наиболее плохо отлажены и нуждаются в оптимизации.

На основе анализа бизнес-процесса предприятия, происходит этап проектирования, где программисты формируют структуру программы и проектируют базу данных (БД).

На этапе реализации, программисты создают базу данных и разрабатывают отдельные компоненты приложения. При окончании разработки отдельного компонента системы, она поставляется клиенту для уточнения требований следующих компонентов. Если есть изменения, то данный компонент дорабатывается, уточняются требования для следующих компонентов и продолжается их разработка. Ключевые этапы этого процесса — простая реализация подмножества требований к программе и совершенствование модели в серии последовательных релизов до тех пор, пока ПО не будет реализовано во всей полноте.

Этап тестирования и отладки подразумевает проведение предварительных испытаний, опытной эксплуатации и приемочных испытаний, которые описаны в Приложении А «Техническое задание».

На этапе ввода в действие необходимо установить серверные и клиентские приложения на рабочие станции, после чего провести окончательное тестирование системы непосредственно на рабочих станциях и убедиться в работоспособности всех компонентов системы.

Для корректной эксплуатации системы следует разработать руководство пользователей и провести инструктаж сотрудников. В соответствии с функционалом внедряемой системы, полномочия некоторых сотрудников могут быть изменены, о чём сотрудники должны быть заранее проинформированы.

Также, создаётся отдельное руководство для администратора системы, так как он несёт наибольшую ответственность за контролем её функционирования и обеспечение.

3.2.2 Ожидаемые риски на этапах ЖЦ и их описание

Хоть инкрементная модель ЖЦ не настолько критична к изменению требований заказчика, по сравнению с каскадной моделью, на этапе анализа необходимо точно определить все каналы информации, которые будут поступать в систему. Если какой-то канал информации будет не учтён, то эффективность ИС сильно снижается.

На этапе проектировании нужно учесть все риски, которые были выявлены на этапе анализа и правильно спроектировать систему. Например, сервер, который анализирует приходящую информацию из источников сообщений, должен отправлять конкретное сообщение только одному эксперту, во избежание дублирование информации в БД.

На этапе реализации необходимо минимизировать возможность совершить пользователю ошибочное действие или предотвратить его, пока эта ошибка не начала влиять на работоспособность системы.

На этапе тестирования и отладки необходимо учесть все сценарии использования ИС, как со стороны администратора ИС, так и со стороны пользователя. Также, необходимо обнаружить нежелательное поведение ИС и устранить его. При тестировании программы, в идеале, её должны опробовать как можно большее количество пользователей.

На этапе внедрение необходимо проконтролировать правильную установку на рабочие станции и использовать только лицензионное ПО для предотвращение несанкционированного доступа.

На этапе эксплуатации необходимо обеспечить правильное и поэтапное обучение персонала и провести контроль знаний по эксплуатации ИС.

3.3 Структура ИС

Контекстная диаграмма ИС в нотации IDEF0 показана на рисунке 8.

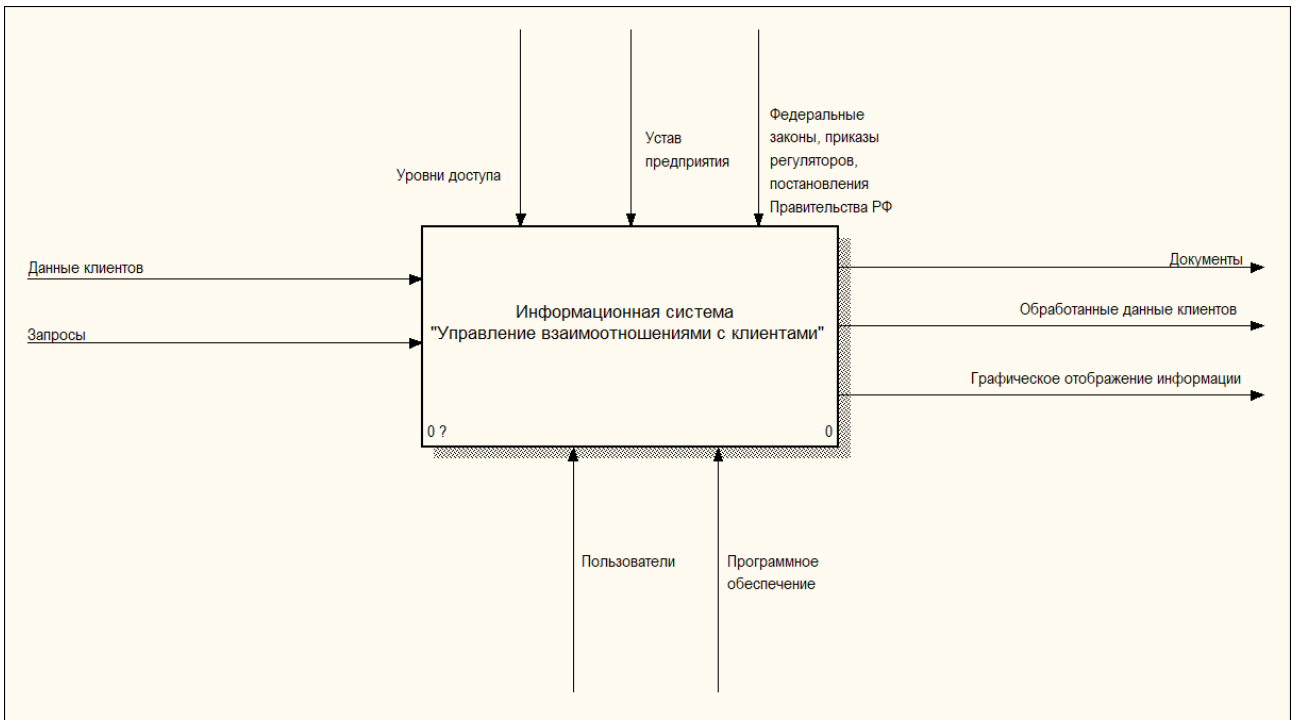

Рисунок 8 – Контекстная диаграмма программы

На вход системы подаются данные клиентов и запросы к базе данных. Выходными данными являются готовые документы, обработанные данные клиентов и графическое отображение информации.

Для визуализации происходящих внутри ИС процессов, необходимо провести декомпозицию контекстной диаграммы. Поскольку в ИС «Управление взаимоотношениями с клиентами» использована клиент-серверная архитектура, первым шагом декомпозиции будет разложение информационной системы на клиентскую часть и серверную. Клиентская часть получает на вход данные клиентов и запросы. Данные клиентов могут передаваться дальше на сервер, либо будут обрабатываться в клиентской части системы и подаваться на выход сразу, либо в виде графического представления. Запросы всегда передаются на сервер. Сервер в свою очередь отвечает на запросы, а также предоставляет в случае необходимости шаблоны документов, которые также хранятся на нём. Клиентская часть, получая шаблоны документов на вход, на выход подаёт готовые документы. Функциональная декомпозиция модели ИС представлена на рисунке 9.

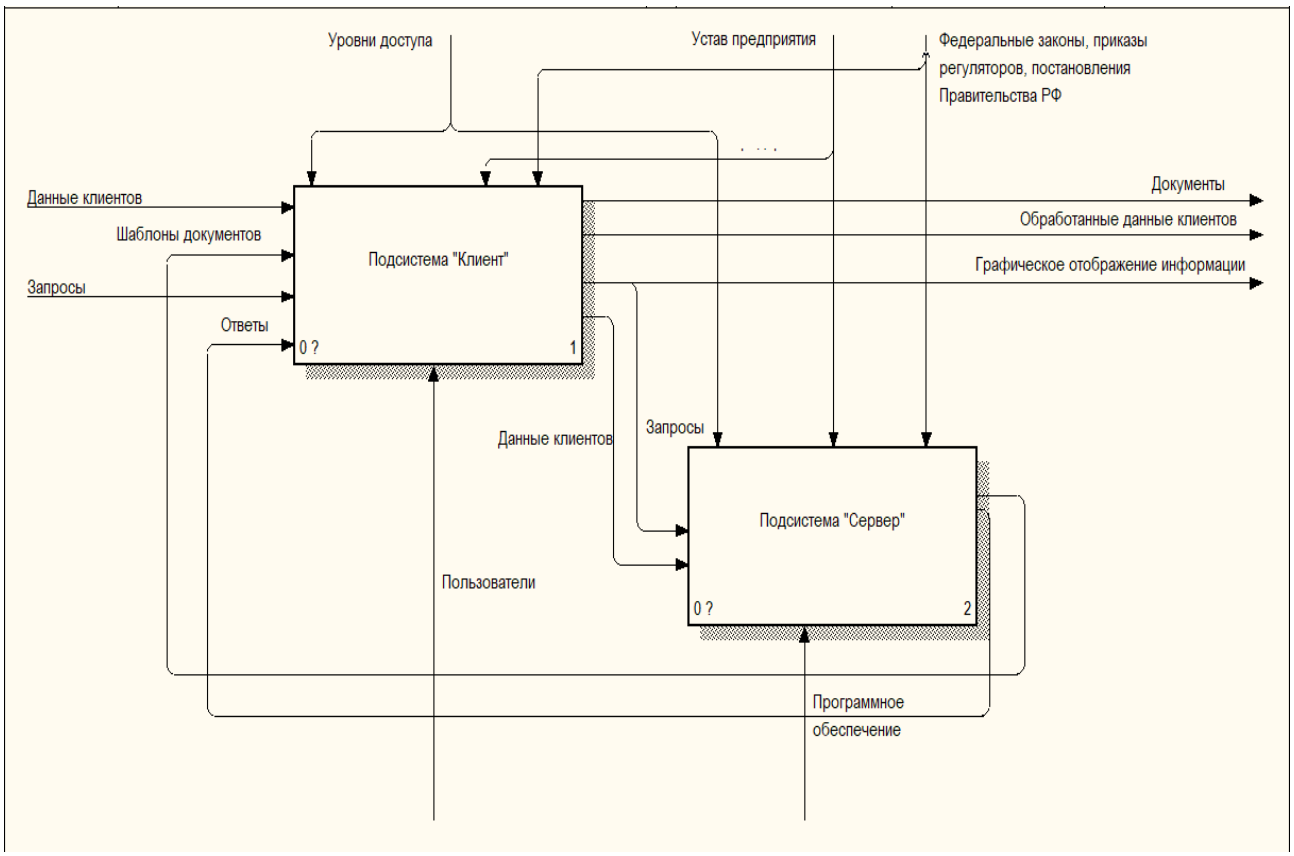

Рисунок 9 – Функциональная декомпозиция модели

Следующий шаг декомпозиции – подробное рассмотрение клиентской и серверной частей как совокупности модулей. В клиентской части присутствуют:

– графический интерфейс, позволяющий принимать данные клиентов и запросы и подавать на выход графическое отображение информации, а также передавать входные данные другим модулям;

– модуль приёма-отправки данных, принимающий ответы сервера, отправляющий на него запросы и полученные данные;

– модуль обработки данных, обрабатывающий входные данные, приводя их к необходимому формату;

– модуль работы с файлами, получающий шаблоны документов с сервера и обработанные данные с модуля обработки данных и подающий на выход готовые документы.

Декомпозиция клиентской части ИС представлена на рисунке 10.

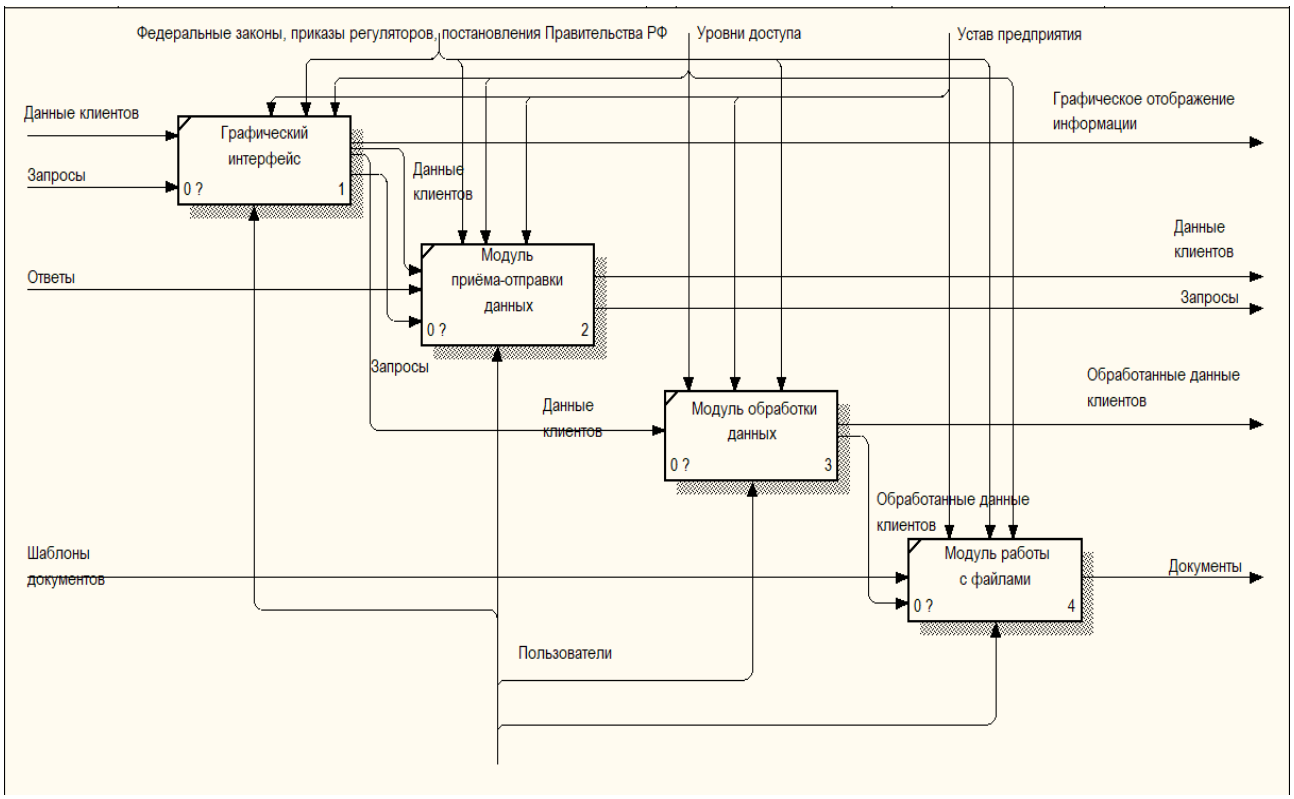

Рисунок 10 – Диаграмма декомпозиции клиентской части ИС

На сервере хранится база данных и шаблоны документов. Диаграмма декомпозиции серверной части представлена на рисунке 11.

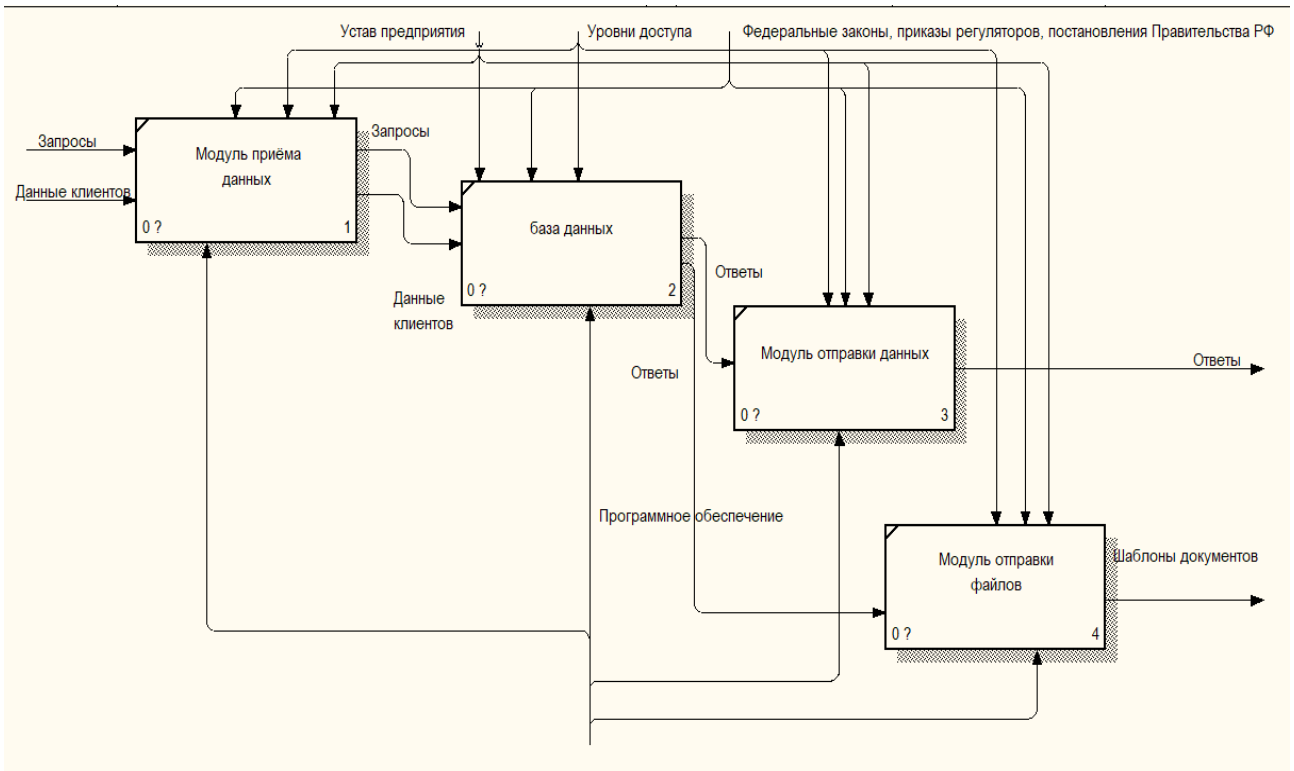

Рисунок 11 – Диаграмма декомпозиции серверной части ИС

В серверной части также присутствуют:

− модуль приёма данных, принимающий запросы с клиента и входные данные и передающий их в базу данных;

− модуль отправки данных, получающий ответы с базы данных и подающий их на выход;

− модуль отправки файлов, получающий ответы с базы данных и подающий на выход шаблоны документов исходя из полученных входных данных.

3.4 Характеристика функциональных подсистем программы

Для начала работы пользователю необходимо авторизоваться путём отправки своих данных на сервер и получения ответа от него. После авторизации пользователю предоставляется основной функционал приложения.

Пользователь может вносить новые данные в базу, создавать документы по шаблонам, делать запросы по базе данных, получать статистику продаж и списки потенциальных покупателей из уже имеющихся в БД клиентов.

На основании перечисленных выше функций можно выделить следующие подсистемы, формирующие структуру ИС:

а) Сервер:

1) Подсистема авторизации – включает в себя идентификацию пользователя и выдачу ему соответствующих прав.

2) Подсистема работы с БД – запись и хранение данных в БД, чтение и изменение этих данных с помощью средств СУБД.

3) Подсистема передачи данных операторам ИС – предоставление некоторых данных по запросу пользователя.

б) Клиент:

1) Подсистема интерфейса пользователя – данная подсистема реализована на стороне клиентского приложения. Основной задачей данной подсистемы является предоставление графического интерфейса, реагирующего на действия пользователя или сообщения от сервера и уведомление пользователя о некорректных действиях или сбоях в работе приложения. Подсистема пользо-

вательского интерфейса не генерирует никаких данных, она лишь получает данные от других подсистем.

2) Подсистема авторизации – обеспечивает функционал по отправке запроса об авторизации на сервер. Поддерживает ожидание ответа об успехе данной операции.

3) Подсистема функционирования клиентской логики – реализует основной функционал по обработке полученных данных от сервера: просмотр данных по запросу, в том числе построение различных вариантов представления статистики. Кроме того, клиент позволяет генерировать документы по шаблонам, получаемым с сервера.

3.5 Проектирование базы данных

При проектировании ИС «Управление взаимоотношениями с клиентами» также была спроектирована и создана база данных.

На основании пяти созданных отношений спроектирована физическая модель, представленная в таблицах 2-6.

Таблица 2 – Физическая структура данных отношения 1 (Сотрудник)

Название атрибута	Тип данных	Условия	Формат данных	Индексация
1	2	3	4	5
ФИО сотрудника	Текст	–	varchar(50)	Primary key
Телефон	Числовой	>0	bigint	–
Должность	Текст	–	varchar(50)	–

Таблица 3 – Физическая структура данных отношения 2 (Позиция)

Название атрибута	Тип данных	Условия	Формат данных	Индексация
1	2	3	4	5
Название	Текстовый	>0	varchar(50)	Primary key
Цена покупки	Числовой	>0	bigint	–
Цена продажи	Числовой	>0	bigint	–
В наличии	Числовой	>=0	bigint	–

Таблица 4 – Физическая структура данных отношения 4 (Договор)

Название атрибута	Тип данных	Условия	Формат данных	Индексация
1	2	3	4	5
Номер договора	Текст	–	varchar(50)	Primary key
Дата заключения	Дата/Время	>01.01.1990	datetime	–
Бюджет	Числовой	>0	bigint	–
Прибыль	Числовой	>=0	bigint	–
Наименование организации	Текст	–	varchar(50)	Foreign key
ФИО сотрудника	Текст	–	varchar(50)	Foreign key

Таблица 5 – Физическая структура данных отношения 5 (Клиент)

Название атрибута	Тип данных	Условия	Формат данных	Индексация
1	2	3	4	5
Наименование организации	Текст	–	varchar(50)	Primary key
ФИО	Текст	–	varchar(50)	–
Телефон	Числовой	>0	bigint	–
Электронная почта	Текст	>0	varchar(50)	–

Таблица 6 – Физическая структура данных отношения 8 (Позиции в договорах)

Название атрибута	Тип данных	Условия	Формат данных	Индексация
1	2	3	4	5
№ Договора	Текст	–	varchar(50)	Foreign key
Название	Текст	–	varchar(50)	Foreign key
Срок действия	Дата/Время	>01.01.1990	datetime	–
Количество	Числовой	>0	bigint	–

Диаграмма базы данных представлена на рисунке 12.

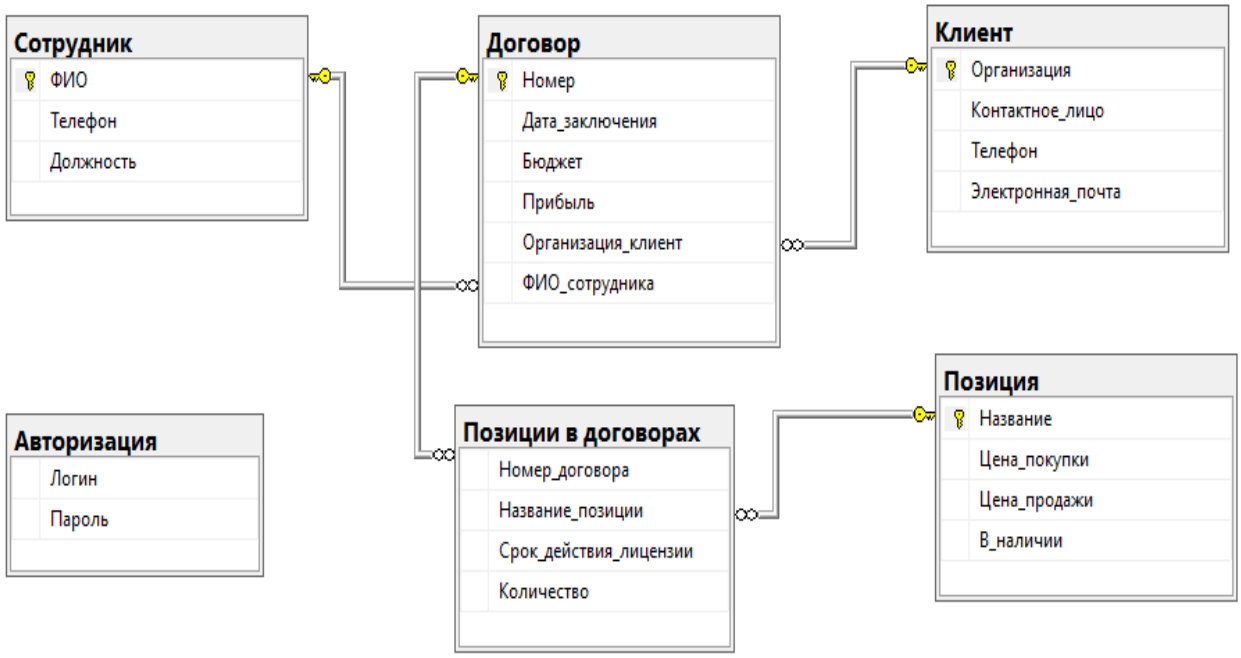

Рисунок 12 – Диаграмма базы данных

На диаграмме помимо представленных 5 отношений присутствует также сущность «Авторизация». Она автономна и участвует только в разграничении доступа к основному массиву данных.

3.6 Задачи автоматизации, решаемые разрабатываемой ИС

При разработке ИС решались следующие задачи, которые подлежали автоматизации:

- сбор и хранение данных о клиентах и их взаимодействии с ООО « СТОЖАРЫ»;
- обработка данных с целью расчёта статистики и планирования задач;
- сортировка данных;
- автозаполнение шаблонов документов.

4 РАЗРАБОТКА ИС УПРАВЛЕНИЯ ВЗАИМООТНОШЕНИЯМИ С КЛИЕНТАМИ

4.1 Средства разработки программы

Во время разработки используется Microsoft SQL Server, Microsoft Visual Studio 2019, Microsoft Windows Presentation Foundation, C# и XAML

Microsoft Visual Studio 2019 выбран по причине того, что программа разрабатывается изначально только для Windows.

Язык C# выбран по причине полной совместимости с остальными средствами разработки, приспособленности его к объектно-ориентированному программированию и удобства.

Язык XAML выбран по причине отсутствия альтернативы при создании графического интерфейса для приложений WPF.

Microsoft Windows Presentation Foundation выбрана в связи с удобством и полной совместимостью с остальными средствами разработки.

Microsoft SQL Server выбран по причине полной совместимости с остальными средствами разработки, наличия бесплатной лицензии и удобства в использовании.

4.2 Архитектура программы

При разработке использовался архитектурный шаблон MVVM, способный в дальнейшем серьёзно облегчить процесс внесения изменений и дополнений в программу, так как он разграничивает логику, логику отображения и отображение. При кажущемся на первый взгляд усложнении проекта, строгое разграничение позволяет ускорить отладку, тестирование, разработку и модификацию, тем самым облегчая рабочий процесс.

Файловая структура проекта представлена на рисунке 13.

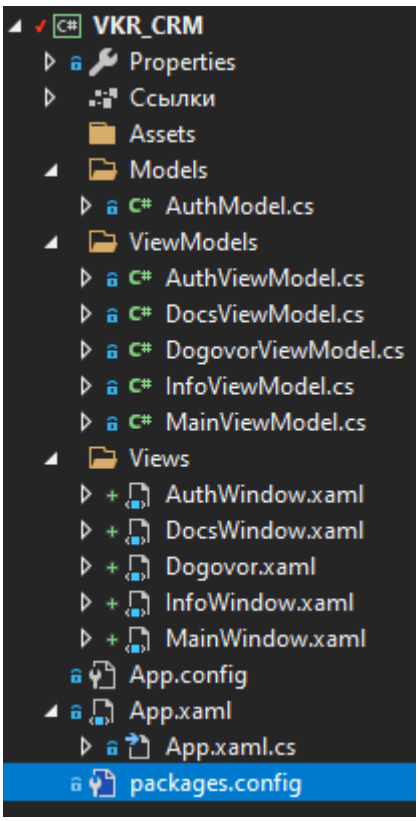

Рисунок 13 – Структура проекта

Согласно данному паттерну при разбиении добавляются новые директории, соответствующие той или иной части паттерна.

4.3 Описание графического интерфейса программы

Графический пользовательский интерфейс разработан при помощи языка разметки XAML и Microsoft WPF и представлен на рисунке 14.

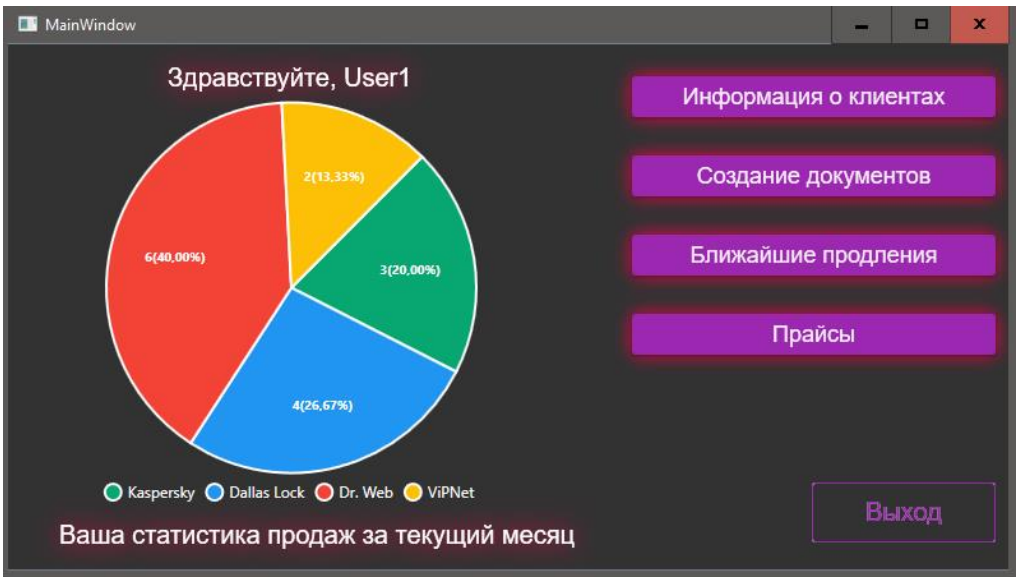

Рисунок 14 – Графический интерфейс главного окна программы

Пользователю во время работы с программой доступны кнопки внесения изменений в БД, просмотра актуальных прайс-листов поставщиков, списка потенциально возможных покупателей из уже внесённых в БД и создание документов по шаблонам. Кроме того, при входе пользователь сразу видит свою статистику по продажам за текущий месяц.

4.4 Описание работы программы

Алгоритм работы программы можно описать следующим образом: пользователь запускает её, осуществляет авторизацию и попадает в главное меню. Форма авторизации представлена на рисунке 15.

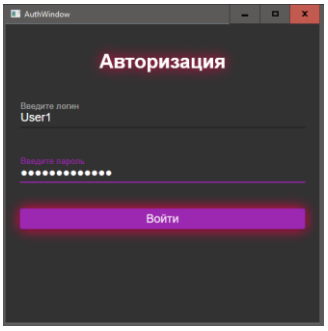

Рисунок 15 – Графический интерфейс формы авторизации

В главном меню в реальном времени отслеживается его статистика продаж, по умолчанию представленная в виде круговой диаграммы. Данные для статистики берутся из БД.

Первая кнопка – «Информация о клиентах» открывает окно поиска по базе данных, которое содержит поле для ввода краткого наименования организации, кнопку «Поиск» и большое текстовое поле, где будут выводиться результаты поиска.

Вторая кнопка – «Создание документов» открывает окно создания документов по шаблонам. На выбор представлено 4 вида документов: договор, коммерческое предложение, спецификация и акт приёма-передачи прав. Графический интерфейс окна создания нового договора представлен на рисунке 16.

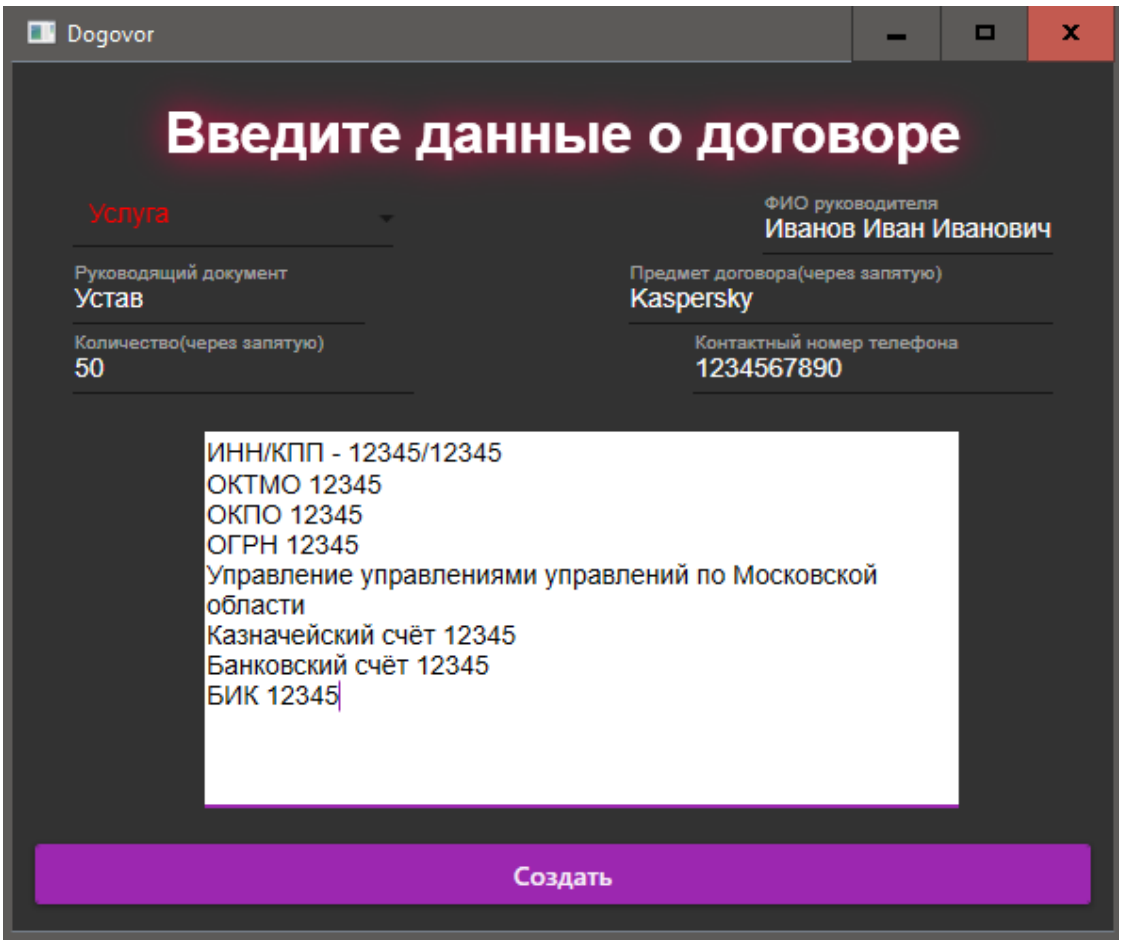

Рисунок 16 – Графически интерфейс окна создания документов

Окно имеет несколько текстовых полей и выпадающих списков для заполнения. Данные с этих полей будут внесены не только в документ, но и в БД. После заполнения всех полей необходимо нажать кнопку «Создать» и документ будет создан в директории приложения на ПК в формате docx/doc.

Третья кнопка на главном окне – «Ближайшие продления» открывает окно, где отображён список организаций, у которых через менее чем месяц окончится срок действия лицензии на ПО. Также показывается наименование истекающего ПО и контактные данные организации.

Четвёртая кнопка – «Прайсы» открывает папку с актуальными прайс-листами поставщиков программного и аппаратного обеспечения.

Последняя кнопка – «Выход» закрывает главное окно и возвращает пользователя к окну авторизации.

5 ИССЛЕДОВАНИЕ И ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ООО «СТОЖАРЫ»

5.1 Типы угроз информационной безопасности

Основными типами угроз информационной безопасности принято считать:

– угрозы по цели воздействия;

– угрозы по характеру воздействия;

– угрозы по характеру возникновения.

Угрозы по цели воздействия также делят на:

− Нарушения конфиденциальности – данная угроза заключается в том, что информация может стать известна тем лицам, у которых нету права к ней. Угроза нарушения конфиденциальности может возникать по вине человека и в следствии работы на компьютере вируса.

− Нарушения целостности – эта угроза связана с изменением информации находящейся в базе данных или на различных носителях. Угроза нарушения целостности также может возникать по вине человека, компьютерного вируса или выхода оборудования из строя

− Нарушения работоспособности – угроза представляет создание условий, из-за которых работоспособность базы данных, информационной системы или программного обеспечения будет невозможна или заблокирована на определенное время. Угроза нарушения работоспособности может быть вызвана различными природными или техногенными явлениями, также нельзя исключать «человеческий фактор» и компьютерные вирусы.

Угрозы по характеру воздействия:

− Активная – при данной угрозе нарушитель может изменить информацию, передаваемую различными способами.

− Пассивная – при данной угрозе нарушитель может только наблюдать информацию, передаваемую различными способами.

Угрозы по расположению угроз:

− Внутренние – источники данной угрозы расположены внутри системы.

− Внешние – источники этой угрозы находятся за периметром системы.

Угрозы по природе возникновения:

− Естественные – угроза этого типа может быть вызвана стихийными природными явлениями или объективными физическими процессами не зависящих от человека

− Искусственные – угрозы, вызванные человеком при его взаимодействии с информацией. Также эти угрозы делят на:

− Непреднамеренные – угрозы, связанные с ошибками в работе программного обеспечения, сотрудников компании, ошибки в работе вычислительной техники.

− Преднамеренные – угрозы, связанные с созданием специального программного обеспечения, которое используется для реализации незаконного доступа к информации, разработка компьютерных вирусов. Данные угрозы вызваны действиями людей.

5.2 Анализ информационной системы «Управление взаимоотношениями с клиентами».

5.2.1 Определение уровня защищенности персональных данных в информационной системе персональных данных «Управление взаимоотношениями с клиентами».

Персональные данные – это любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу или юридическому лицу.

В соответствии с требованиями постановления Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» был проведен анализ исходных данных объекта информатизации – информационной системы персональных данных «Управление взаимоотношениями с клиентами» с целью определения основных критериев, влияющих на выбор уровня защищенности персональных данных.

При анализе учитывались характеристики персональных данных субъектов персональных данных, их количество, принадлежность субъектов персональных данных к числу работников организации оператора, тип угроз безопасности персональных данных.

При анализе исходных данных было установлено:

– для информационной системы актуальными угрозами следует считать угрозы 3-го типа, не связанные с наличием недокументированных (незадекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе;

– в информационной системе обрабатываются персональные данные лиц, не являющихся сотрудниками оператора;

– в информационной системе обрабатываются иные категории персональных данных менее чем 100 000 субъектов персональных данных, не являющихся сотрудниками оператора.

На основании проведенного анализа было установлено что информационная система персональных данных «Управление взаимоотношениями с клиентами» обеспечивает 4-й уровень защищенности персональных данных.

5.2.2 Исходный уровень защищенности информационной системы персональных данных

Под уровнем исходной защищенности информационной системы персональных данных рассматривается обобщенный показатель, зависящий от технических и эксплуатационных характеристик информационной системы персональных данных (Y_1). Характеристики информационной системы «Управление взаимоотношениями с клиентами» показаны в таблице 7.

Таблица 7 – Показатели информационной системы «Управление взаимоотношениями с клиентами».

Технические и эксплуатационные характеристики	Уровень защищенности
1	2
По территориальному размещению (локальная ИСПДн, развернутая в пределах одного здания)	Высокий

Продолжение таблицы 7

1	2
По наличию соединения с сетями общего пользования (ИСПДн, имеющая одноточечный выход в сеть общего пользования)	Средний
По встроенным (легальным) операциям с записями баз персональных данных (модификация, передача)	Низкий
По разграничению доступа к персональным данным (ИСПДн, к которой имеют доступ определенные перечнем сотрудники организации, являющейся владельцем ИСПДн, либо субъект ПДн)	Средний
По наличию соединений с другими базами ПДн иных ИСПДн (ИСПДн, в которой используется одна база ПДн, принадлежащая организации – владельцу данной ИСПДн)	Высокий
По уровню (обезличивания) ПДн (ИСПДн, в которой предоставляемые пользователю данные не являются обезличенными (т.е. присутствует информация, позволяющая идентифицировать субъекта ПДн)	Низкий
По объему ПДн, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки (ИСПДн, предоставляющая часть ПДн)	Средний

ИСПДн имеет средний уровень исходной защищенности, так как не менее 70% характеристик ИСПДн соответствуют уровню не ниже «средний».

Показатель исходной защищенности Y_1 =5.

5.2.3 Вероятность реализации угроз безопасности персональных данных

Под вероятностью реализации угрозы рассматривается показатель, определяемый экспертным путем, характеризующий, насколько возможна реализация конкретной угрозы безопасности персональных данных для ИСПДн.

Числовой коэффициент (Y_2) для оценки вероятности возникновения угрозы определяется по 4 вербальным градациям показателя согласно Таблице 8.

Таблица 8 – Оценки вероятности возникновения угрозы

Показатель	Описание	Значение Y_2
1	2	3
Маловероятно	отсутствуют объективные предпосылки для осуществления угрозы	$Y_2 = 0$
Низкая вероятность	объективные предпосылки для реализации угрозы существуют, но принятые меры существенно затрудняют ее реализацию	$Y_2 = 2$

Продолжение таблицы 8

1	2	3
Средняя вероятность	объективные предпосылки для реализации угрозы существуют, но принятые меры обеспечения безопасности ПДн недостаточны	$Y_2 = 5$
Высокая вероятность	объективные предпосылки для реализации угрозы существуют и меры по обеспечению безопасности ПДн не приняты	$Y_2 = 10$

5.2.4 Реализуемость угроз

По результатам оценки уровня защищенности (Y_1) и вероятности реализации угрозы (Y_2), рассчитывается коэффициент реализуемости угрозы (Y) и определяется возможность реализации угрозы. Коэффициент реализуемости угрозы Y будет определяться соотношением $Y = (Y_1 + Y_2)/20$.

По значению коэффициента реализуемости угрозы Y формируется вербальная интерпретация реализуемости угрозы следующим образом:

– если $0 \leq Y \leq 0,3$ то возможность реализации угрозы признается низкой;

– если $0,3 < Y \leq 0,6$ то возможность реализации угрозы признается средней;

– если $0,6 < Y \leq 0,8$ то возможность реализации угрозы признается высокой;

– если $Y > 0,8$ то возможность реализации угрозы признается очень высокой.

5.2.5 Оценка опасности угроз

Оценка опасности угроз безопасности персональных данных составляется на основе опроса экспертов по защите информации и определяется вербальным показателем опасности, который имеет три значения:

низкая опасность - если осуществление угрозы может причинить незначительные неблагоприятные последствия для субъекта персональных данных;

средняя опасность - если осуществление угрозы может причинить неблагоприятные последствия для субъекта персональных данных;

высокая опасность - если осуществление угрозы может причинить значительные неблагоприятные последствия для субъекта персональных данных.

С учетом обрабатываемых категорий персональных данных и прочих характеристик, ИСПДн является информационной системой, для которой нарушение конфиденциальности и/или целостности и/или доступности информации, обрабатываемой в ней, может причинить незначительные неблагоприятные последствия для субъекта персональных данных.

5.2.6 Определение актуальности угроз в информационной системе персональных данных

Согласно правилам отнесения угрозы безопасности к актуальной, для ИСПДн определяются актуальные и неактуальные угрозы. Правила определения актуальности УБПДн представлены в таблице 9.

Таблица 9 – Правила определения актуальности УБПДн

Возможность реализации угрозы	Показатель опасности угрозы		
	Низкая	Средняя	Высокая
Низкая	неактуальная	неактуальная	актуальная
Средняя	неактуальная	актуальная	актуальная
Высокая	актуальная	актуальная	актуальная
Очень высокая	актуальная	актуальная	актуальная

5.2.7 Оценка угроз безопасности персональных данных в информационной системе «Управление взаимоотношениями с клиентами»

Состав угроз определен следующим образом. На основе «Базовой модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных» установлена типовая модель угроз безопасности, актуальная для организации: Типовая модель угроз безопасности персональных данных, обрабатываемых в распределенных информационных системах персональных данных, имеющих подключение к сетям связи общего пользования и(или) сетям международного информационного обмена. Для данной

типовой модели возможна реализация следующих УБПДн (таблица Б.1 – Угрозы и их характеристики. Приложение Б).

5.3 Состав и содержание мер по обеспечению безопасности персональных данных в ИСПДн «Управление взаимоотношениями с клиентами»

Состав и содержание мер по обеспечению безопасности персональных данных в информационной системе персональных данных «Управление взаимоотношениями с клиентами» для обеспечения 4-го уровня защищённости персональных данных показаны в таблице 10:

Таблица 10 – Состав и содержание мер по обеспечению безопасности персональных данных.

Условное обозначение меры	Содержание мер по обеспечению безопасности персональных данных
1	2
I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)	
ИАФ.1	Идентификация и аутентификация пользователей, являющихся работниками оператора
ИАФ.3	Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов
ИАФ.4	Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации
ИАФ.5	Защита обратной связи при вводе аутентификационной информации
ИАФ.6	Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей)
II. Управление доступом субъектов доступа к объектам доступа (УПД)	
УПД.1	Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей
УПД.2	Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа
УПД.3	Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами
УПД.4	Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы
УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы

Продолжение таблицы 10

1	2
УПД.6	Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе)
УПД.13	Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети
УПД.14	Регламентация и контроль использования в информационной системе технологий беспроводного доступа
УПД.15	Регламентация и контроль использования в информационной системе мобильных технических средств
УПД.16	Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы)
V. Регистрация событий безопасности (РСБ)	
РСБ.1	Определение событий безопасности, подлежащих регистрации, и сроков их хранения
РСБ.2	Определение состава и содержания информации о событиях безопасности, подлежащих регистрации
РСБ.3	Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения
РСБ.7	Защита информации о событиях безопасности
VI. Антивирусная защита (АВЗ)	
АВЗ.1	Реализация антивирусной защиты
АВЗ.2	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)
VIII. Контроль (анализ) защищенности персональных данных (АНЗ)	
АНЗ.2	Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации
XII. Защита технических средств (ЗТС)	
ЗТС.3	Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы, в помещения и сооружения, в которых они установлены
ЗТС.4	Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр
XIII. Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)	
ЗИС.3	Обеспечение защиты персональных данных от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи

5.4 Способы и средства защиты информации и защиты персональных данных в ИСПДн «Управление взаимоотношениями с клиентами»

5.4.1 Способы защиты информации

– Ограничение пользователей в помещения, в которых расположены средства обработки и хранения информации содержащую ПДн;

– Разграничение прав пользователей к средствам обработки и защиты информации, информационным ресурсам;

– Регистрация и хранение съемных носителей информации;

– Применение средств защиты, прошедших сертификацию в специализированных органах сертификации;

– Использование защищённых каналов связи;

– Расположение технических средств, обрабатывающих информацию содержащую персональные данные в пределах охраняемой территории;

– Создание физической защиты помещений и технических устройств, обрабатывающих информацию, содержащую ПДн;

– Недопущение установки в ИС вредоносных программ (вирусов).

5.4.2 Программные и технические средства защиты информации

В ИСПДн «Управление взаимоотношениями с клиентами» необходимо использовать программы, сертифицированные Федеральной службой по техническому и экспортному контролю (ФСТЭК России).

Для обеспечения безопасности персональных данных в ИСПДн 4 уровня защищенности следует использовать следующие программные и технические средства защиты информации:

1. Для обеспечения защиты базы данной и исходного кода на сервере компании следует использовать сертифицированный аппаратный межсетевой экран и сертифицированное антивирусное средство защиты на сервере.

2. Для обеспечения защиты информации на пользовательских рабочих местах необходимо использовать средства защиты информации от несанкционированного доступа с межсетевым экраном и антивирусное средство защиты.

На данный момент для защиты информации в компании ООО «СТОЖАРЫ» используют:

– На данный момент на сервере компании ООО «СТОЖАРЫ» установлен сертифицированный аппаратный межсетевой экран и антивирус «Kaspersky Security for Windows Server»

На данный момент, на пользовательских компьютерах установлен антивирус «Kaspersky Endpoint Security», для компьютеров на которых будут обрабатываться персональные данные, также установлено средство защиты информации от несанкционированного доступа.

6 БЕЗОПАСНОСТЬ ЖИЗНЕДЕЯТЕЛЬНОСТИ

6.1 Безопасность

6.1.1 Анализ эргономики программы

Эргономичность – наибольшая производительность при наименьшей вероятности ошибки при работе с программой.

Система управления взаимоотношениями с клиентами – программный продукт, разрабатываемый в рамках выпускной квалификационной работы бакалавра. Назначением данного продукта является упрощение бизнес-процесса предприятия и повышение эффективности его деятельности.

Критериями для оценки эргономичности программы можно считать:

- сложность обучения;

- интуитивную воспринимаемость графического интерфейса, выражающуюся в совпадении между изображением в интерфейсе и предполагаемым действием;

- цену ошибки, принимаемую как стоимость ошибки, произошедшей по вине пользователя, как например, некорректный ввод или неверные действия пользователя.

Интуитивная воспринимаемость графического интерфейса и скорость обучения напрямую связаны. Если графический интерфейс будет непонятен пользователю или не будет соответствовать функциональному назначению, пользователь будет вынужден тратить дополнительное время на обучение работе с программным продуктом.

Цена ошибки может быть определена как количество возникающих ошибок и их стоимость. Цену ошибки можно оценить как минимальную, по причине того, что в случае ввода некорректных данных, ошибочных действий со стороны пользователя, исходные данные никак не будут затронуты и не будут испорчены. Пользователь в таком случае имеет возможность исправить некорректные данные. Стоит отметить, что в случае возникновения ошибки или при вводе некорректных данных, сотрудник тратит дополнительное время на ис-

правления, но временные затраты достаточно малы, чтобы ими можно было пренебречь.

Для минимизации возможных ошибок, интерфейс программы не подразумевает большое количество активных элементов, например, кнопки и переключатели. На главном окне, показанном на рисунке 17, можно отметить наличие 4 кнопок и 1 круговой диаграммы. В случае попытки добавления пустых строк в базу, программа не даст выполнить данное действие, предупредив пользователя о том, что обязательные для заполнения строки пусты.

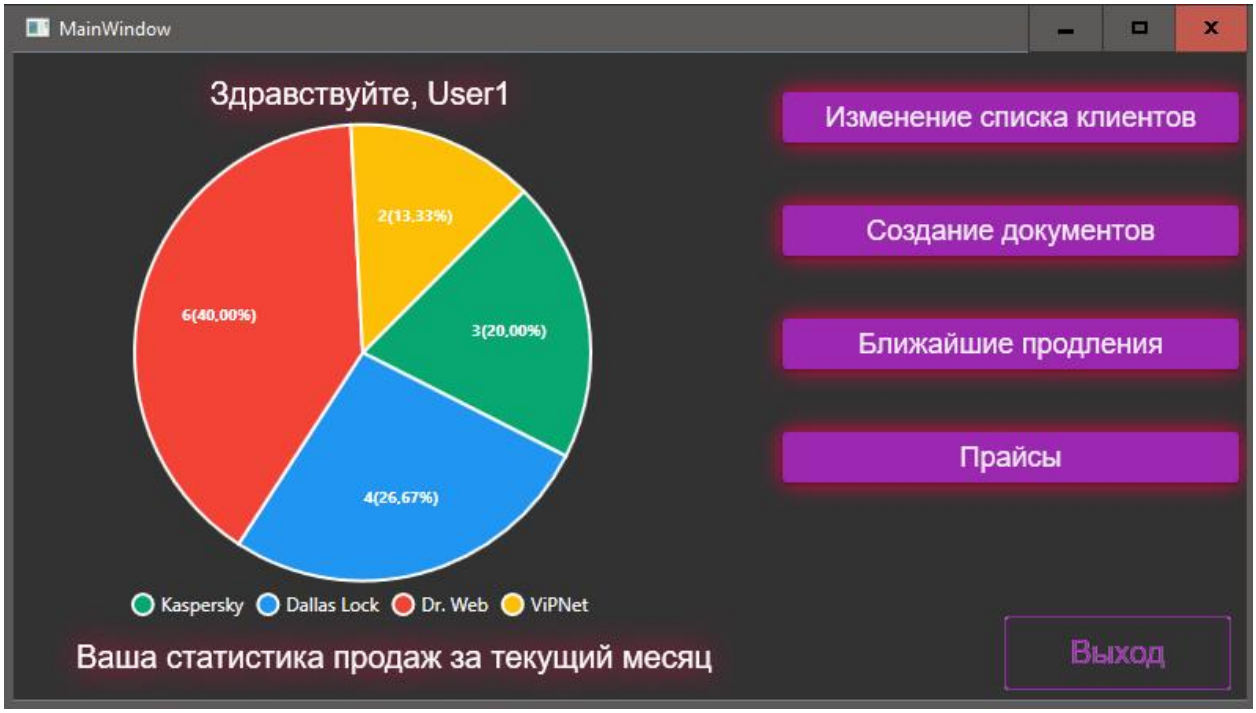

Рисунок 17 – Главное окно CRM-системы

Все кнопки подписаны и выполняют ровно то, о чём на них объявлено, что позволяет сделать интерфейс программы интуитивно понятным.

Исходя из вышесказанного можно утверждать, что *цена ошибки* для данного программного продукта минимальна, *интуитивная воспринимаемость графического интерфейса* оценивается как интуитивно понятна, потому что в интерфейсе изображение соответствует назначению, а *сложность обучения* работе с данным программным продуктом является низкой, потому что пользователю доступно минимальное количество элементов управления.

6.1.2 Анализ опасных и вредных факторов на рабочем месте пользователя ЭВМ

Данная программа рассчитана на использование только на ЭВМ, что подразумевает необходимость в анализе рабочего места пользователя с ЭВМ.

Работа за ЭВМ подразумевает работу в сидячем положении. Рабочее место для работы в сидячем положении должно соответствовать требованиям, описанным пунктом 6.3 СП 2.22.3670-20, а именно:

- пространство для размещения ног высотой не менее 600 мм;
- на уровне колен глубина не менее 450 мм;
- на уровне стоп глубина не менее 600 мм;
- шириной не менее 500 мм.

Площадь одного рабочего места пользователя ПЭВМ с использованием плоских дискретных экранов обозначена в пункте 249 СП 2.2.3670-20 и составляет не менее 4,5 кв.м.

ПЭВМ необходимо размещать таким образом, чтобы показатели освещенности не превышали установленных в СанПин 1.2.3685-21 таблице 5.23 норм, согласно пункту 251 СП 2.2.3670-20. К рабочему месту предъявлены требования площади рабочей поверхности более 0,1 кв.м. наибольшая допустимая яркость равняется 500 кд/кв.м.

6.2 Экологичность

Экологичность – качество чего-либо, отражающее его способность не наносить вреда окружающей природе. Отходы производства – вещества или предметы, которые образованы в процессе производства, выполнения работ, оказания услуг или в процессе потребления, которые удаляются, предназначены для удаления или подлежат удалению. Удаление или утилизация отходов – главная задача, поставленная перед предприятием для обеспечения экологической безопасности окружающей среды. Это трудоемкий и сложный процесс, для которого необходим обученный специальным образом и хорошо подготовленный персонал, состоящий из специалистов, способных должным образом утилизировать тот или иной вид отходов.

Каждое предприятие должно обеспечить уничтожение отходов. Утилизация отходов должна соответствовать необходимым нормам и стандартам, несоблюдение которых может повлечь за собой получение предприятием серьезных штрафов и санкций, а также закрытие работы предприятия.

Организация, производящая какой-либо продукт, производит отходы, указанные в ГОСТ 30772-2001:

− вторичная продукция – вещества, материалы, комплектующие изделия, детали, функциональные узлы, блоки, агрегаты от различных объектов, утратившие свои потребительские свойства и не пригодные для дальнейшей эксплуатации в соответствии с директивными требованиями и/или нормативной документацией, но представляющие собой товарную продукцию.

− отходы производства – остатки сырья, материалов, веществ, изделий, предметов, образовавшиеся в процессе производства продукции, выполнения работ (услуг) и утратившие полностью или частично исходные потребительские свойства.

К вторичной продукции, в организации использующей ЭВМ, можно отнести комплектующие ЭВМ и периферию.

Возможна переработка объектов, состоящих преимущественно из пластмасс. Объекты микроэлектроники, не подлежащие переработке, отправляются на вторичное использование.

Возможна продажа вторичной продукции как товаров бывших в употреблении. Тогда организации получает возможность окупить некоторые объекты производства, не затрачивая ресурсов на утилизацию.

Отходы производства подлежат только утилизации. Для утилизации отходы производства сортируются по типу материала, после чего отправляются в центры утилизации, которые утилизируют отходы в соответствии с необходимыми требованиями.

6.3 Безопасность при возникновении чрезвычайных ситуаций

Пожар является одной из самых распространенных чрезвычайных ситуаций на предприятиях. Основными причинами возникновения пожара считают-

ся: неосторожное обращение с огнем или легко воспламеняемыми веществами вблизи открытых источников огня, курение в неустановленных для этого местах, оставленные без присмотра электроприборы и использование электроприборов с неисправностью, пренебрежительное отношение к правилам пожарной безопасности и т.д.

Согласно НПБ 105-03, помещения с ЭВМ являются пожароопасными в категории В1 – В4, в которых могут содержаться материалы, способные гореть при взаимодействии с водой или друг другом. Все провода должны быть спрятаны в кабель-каналы или стены, а путь эвакуации не должен быть загорожен мебелью или другими объектами.

Для предотвращения пожара нужно соблюдать следующие правила:

- не хранить и не применять горючие жидкости, взрывчатые вещества, баллоны с газами рядом с ЭВМ;
- не использовать электронагревательные приборы;
- не эксплуатировать провода электроприборов с поврежденной изоляцией;
- не пользоваться поврежденным электрооборудованием и розетками;
- не накрывать светильники и бытовые приборы горючими материалами;
- не курить в помещении;
- оставлять без наблюдения включенную в сеть ПЭВМ;
- не пользоваться неисправной аппаратурой;
- не разрешается ремонтировать блоки ЭВМ непосредственно в помещениях, где они располагаются;
- не нарушать правила эксплуатации ПЭВМ;
- раз в 3 месяца необходимо проводить санитарную очистку.

По окончании работы необходимо обесточить все электроприборы, осмотреть помещения на наличие признаков возгорания, а также необходимо выключить автомат питания в распределительном щите.

Если случилось возгорание, необходимо позвонить в пожарную службу, сообщить всю необходимую информацию, подготовить к эвакуации материальные ценности, документацию и покинуть здание через запасные выходы. Если нет возможности покинуть здание, то необходимо закрыться в менее задымлённой комнате, не дать дыму попадать в комнате любыми подручными средствами и открыв все окна ожидать помощи спасательной бригады.

6.4 Физические упражнения и рекомендации при работе за ЭВМ

Слишком большое количество времени, проводимого за компьютером, приводит к высокой нагрузке как на опорно-двигательный, так и на зрительный аппараты человека. Поначалу проблема может быть незаметна, однако постепенно формируются такие серьезные нарушения как: снижение зрения, искривление осанки и артрит. В целях профилактики рекомендуется выполнять комплекс упражнений для снятия усталости, а также соблюдать рекомендации, предназначенные для комфортной работы за ЭВМ и сохранения здоровья пользователя ЭВМ..

В качестве рекомендаций при работе с ЭВМ стоит отметить:

- Дистанция между монитором и глазами должна быть не менее 45 см и не более 70 см.
- Клавиатуру и экран следует располагать прямо перед собой, чтобы минимизировать повороты.
- Голову необходимо держать прямо, а руки необходимо располагать на клавиатуре так, чтобы запястья были расслаблены.
- Спину следует держать ровной.
- Необходимо делать периодический отдых. Раз в час следует вставать с рабочего места и делать перерыв. Не лишним будет выполнение гимнастики, прогулки по помещению или выход на улицу для прогулки. Необходимо снимать напряжение с глаз, потому что работа за компьютером подразумевает частое напряжение зрительного органа человека.

Упражнения для снятия усталости с кистей рук и плечевого пояса.

а) Упражнение можно выполнять как сидя, так и стоя. Левую руку вытянуть вперед, правую поднять вверх. Меняем положения рук, поочередно. Темп выполнения средний.

б) Положение стоя. Руки тыльной стороной кисти прижать к поясу. Свести локти вместе голову наклонить вперед. Локти развести в стороны и пытаться свести за спиной, голову наклонить назад.

в) Выполнять сидя на стуле. Поднять руки вверх сжимать и разжимать поочередно кисти рук.

Упражнения для снятия напряжения с туловища.

а) Исходное положение – стоя, руки за голову, ноги чуть шире плеч. Поворачивать таз влево и вправо. Плечевой пояс неподвижен.

б) Положение аналогично первому упражнению. Круговые вращения тазом по часовой стрелке и против часовой стрелки, поочередно.

в) Исходное положение – ноги врозь. Наклон вперед, правая рука скользит по ногам вниз, а левая поднимается вдоль тела. Далее – то же самое, со сменой положения рук.

Упражнения для улучшения кровообращения в мозговой области.

а) Исходное положение на стуле, руки свесить, расслабиться. Медленный наклон головы назад. Медленно считаем до трех. Принимаем исходное положение. Медленно наклоняем голову вперед. Считаем до трех и возвращаемся в исходное положение.

б) Исходное положение – сидя на стуле, руки на поясе. Делаем всё как в первом упражнении, но голову наклоняем поочерёдно к плечам.

в) Выполнять сидя или стоя. Левую руку заносим за голову и тянемся к правому плечу, поворачиваем голову налево. Считаем до трех и проделываем все то же самое, но с правой рукой и голову поворачиваем направо.

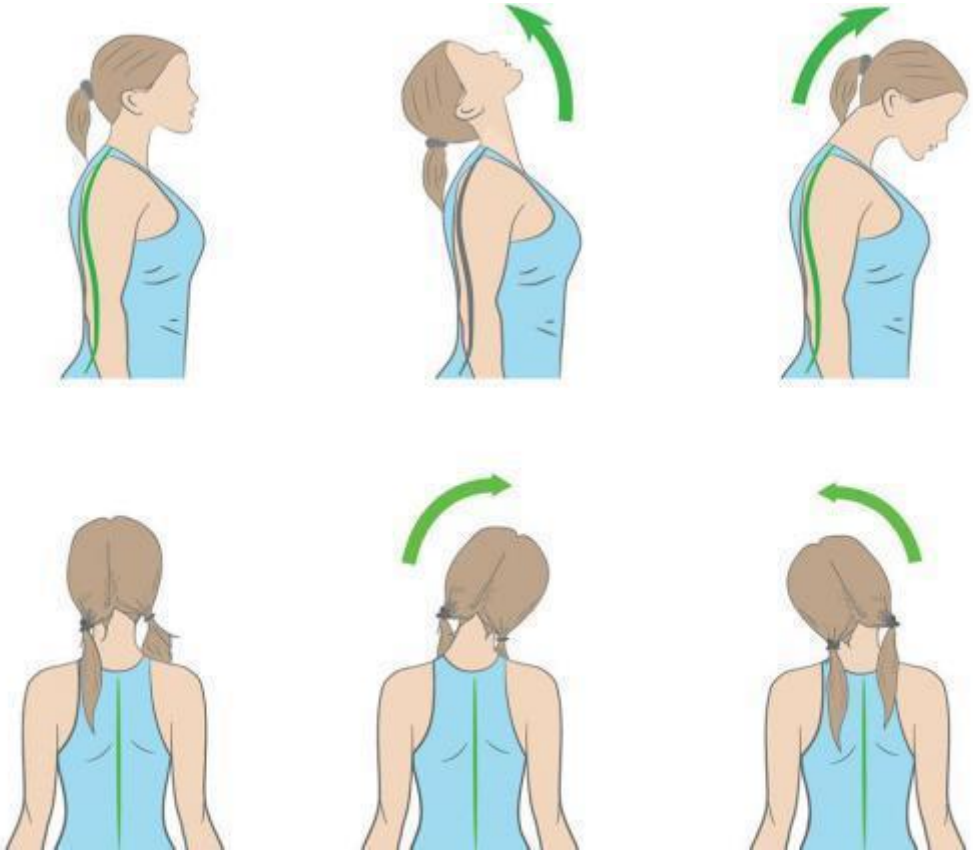

Рисунок 18 – Иллюстрация упражнений для шейного отдела

ЗАКЛЮЧЕНИЕ

На сегодняшний день для малых коммерческих предприятий особо остро стоит проблема автоматизации работы и упрощения основных бизнес-процессов. В особенности это касается предприятий, занятых в сфере IT.

Система управления взаимоотношениями с клиентами позволяет решить эту проблему наиболее безболезненным способом – весь функционал сосредоточен в одной программе.

В ходе выполнения бакалаврской работы был осуществлён анализ существующих CRM-систем, выявлены их основные недостатки (недружелюбность к пользователю, громоздкость, небезопасность и высокая цена). На основании анализа были определены требования к разработке, изложенные в техническом задании в приложении А.

В работе рассмотрены и описаны необходимые функциональные модули системы, описана структура и алгоритмы работы модулей ИС.

Проект реализован средствами: Microsoft WPF, языков XAML и C#, Microsoft Visual Studio 2019 и Microsoft SQL Server.

Для разработанной информационной системы проведён анализ информационной безопасности, безопасности жизнедеятельности и экологичности, даны рекомендации по работе за персональной ЭВМ.

Разработанная ИС позволяет хранить, изменять, удалять, добавлять данные о клиентах в БД; быстро создавать документы по шаблонам; в реальном времени отслеживать статистику продаж, иметь быстрый доступ к актуальным ценам у поставщиков, а так же разработанная ИС решает некоторые задачи планирования, выводя список ближайших запланированных продлений лицензий программного обеспечения у имеющихся в базе клиентов.

В настоящее время разработанная ИС проходит тестирование в организации ООО «СТОЖАРЫ». Планируется её внедрение в деятельность указанной организации.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1 Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (Утверждена Заместителем директора ФСТЭК России 15 февраля 2008 г.). . [Электронный ресурс]: URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/379-bazovaya-model-ugroz-bezopasnosti-personalnykh-dannykh-pri-ikh-obrabotke-v-informatsionnykh-sistemakh-personalnykh-dannykh-vypiska-fstek-rossii-2008-god (дата обращения: 19.05.2022).

2 Гаврилов, М. В. Информатика и информационные технологии : учебник для вузов / М. В. Гаврилов, В. А. Климов. — 4-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2022. — 383 с. — (Высшее образование). — ISBN 978-5-534-00814-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/488708 (дата обращения: 13.02.2022).

3 Гринберг, П. CRM со скоростью света. Привлечение и удержание клиентов в реальном времени через Интернет / Гринберг П.: [пер. с англ. В. Агапов]. - 3-е изд. – Санкт-Петербург : Издательство Символ-Плюс 2018. – 530 с.

4 Документация по языку программирования C# [Электронный ресурс]: URL: https://docs.microsoft.com/ru-RU/dotnet/csharp/ (дата обращения: 04.06.2022).

5 Зыков, С. В. Программирование. Объектно-ориентированный подход : учебник и практикум для вузов / С. В. Зыков. – Москва : Издательство Юрайт, 2022. — 155 с. – (Высшее образование). – ISBN 978-5-534-00850-0. – Текст : электронный // Образовательная платформа Юрайт [сайт]. – URL: https://urait.ru/bcode/490423 (дата обращения: 01.04.2022).

6 Коннолли, Т. Базы данных. Проектирование, реализация и сопровождение. Теория и практика / Т. Коннолли. – Москва.: Издательский дом «Вильямс», 2008. – 1120 с.

7 Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. ФСТЭК России, 2008 г. [Электронный ресурс]: URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/380-metodika-opredeleniya-aktualnykh-ugroz-bezopasnosti-personalnykh-dannykh-pri-ikh-obrabotke-v-informatsionnykh-sistemakh-personalnykh-dannykh-fstek-rossii-2008-god (дата обращения: 19.05.2022).

8 О персональных данных [Электронный ресурс]: федеральный закон: [принят Государственной Думой 8 июля 2006 г.: одобрено Советом Федерации 14 июля 2006 г.]. – Режим доступа: http://www.consultant.ru/document/Cons_doc_LAW_61801/ (дата обращения: 26.05.2022).

9 Об информации, информационных технологиях и о защите информации. [Электронный ресурс]: федеральный закон от 27 июля 2006 г.: «URL: https://docs.cntd.ru/document/901990051 (дата обращения: 04.06.2022).

10 Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных [Электронный ресурс]: Приказ ФСТЭК России от 18 февраля 2013 г. URL: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/691-prikaz-fstek-rossii-ot-18-fevralya-2013-g-n-21 (дата обращения: 19.05.2022).

11 Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных [Электронный ресурс]: Постановление Правительства РФ от 01.11.2012 URL: http://pravo.gov.ru/proxy/ips/?docbody=&nd=102160483 (дата обращения: 04.06.2022).

12 Руководство по работе с Microsoft SQL Server [Электронный ресурс]: URL: https://docs.microsoft.com/ru-ru/sql/?view=sql-server-ver16 (дата обращения: 04.06.2022).

13 Руководство по WPF [Электронный ресурс]: URL: https://docs.microsoft.com/ru-ru/dotnet/desktop/wpf/?view=netframeworkdesktop-4.8 (дата обращения: 04.06.2022).

14 Сайт компании ООО «СТОЖАРЫ» [Электронный ресурс]: URL: http://stogary.ru/ (дата обращения: 01.06.2022).

15 Сайт о программировании Metanit.com [Электронный ресурс]: Руководство по WPF URL: https://metanit.com/sharp/wpf/ (дата обращения: 04.06.2022).

16 Сайт Хабр [Электронный ресурс]: Понимание XAML URL: https://habr.com/ru/post/141069/ (дата обращения: 04.06.2022).

17 Сайт Professor Web [Электронный ресурс]: Паттерн MVVM URL: https://professorweb.ru/my/WPF/documents_WPF/level36/36_5.php (дата обращения: 04.06.2022).

18 Троелсен, Э.. Язык программирования C# 7 и платформы .NET и .NET Core / Э. Троелсен, Ф. Джепикс ; [пер. с англ. Ю.Н. Артеменко] . – 8-е изд. – Вильямс, 2018. – 1328 с.

19 Шаньгин, В.Ф. Информационная безопасность компьютерных систем и сетей: учеб. пособие. / В. Ф. Шаньгин. − М.: ИД «ФОРУМ»: ИНФРА-М, 2019. − 416 с.

20 MVVM – Краткое руководство [Электронный ресурс]: URL: https://coderlessons.com/tutorials/microsoft-technologies/vyuchit-mvvm/mvvm-kratkoe-rukovodstvo (дата обращения: 04.06.2022).

ПРИЛОЖЕНИЕ А

УТВЕРЖДАЮ
Исполнительный директор
ООО «СТОЖАРЫ»
_____Ю.А. Кравчина
«15» 06 2022 г.

Техническое задание

1 ОБЩИЕ СВЕДЕНИЯ

1.1 Полное наименование приложения

Информационная система «Управление взаимоотношениями с клиентами».

1.2 Область применения

Программа предназначена для упрощения основных бизнес-процессов предприятия-заказчика и повышения эффективности его работы.

1.3 Наименование предприятий исполнителя и заказчика системы

Исполнитель: студент группы 855-об, факультета математики и информатики, Амурского государственного университета Сенашов Егор Тимофеевич.

Заказчик: Общество с ограниченной ответственностью «СТОЖАРЫ»

Фактический адрес: 675000, Амурская область, г. Благовещенск, ул. Батарейная, 26/4

1.4 Перечень документов

Документы, на основании которых создается ИС предприятия:

– ГОСТ 34.601-90 – техническое задание на проектирование автоматизированной системы управления;

– ГОСТ 34.602-89 – техническое задание.

1.5 Плановые сроки начала и окончания работы

Срок начала работ: 7 февраля 2022 года.

Срок окончания работ: 21 июня 2022 года.

1.6 Сведения об источниках и порядке финансирования работ

Данный проект является учебным и выполняется без привлечения каких-либо финансовых средств.

Продолжение ПРИЛОЖЕНИЯ А

2 НАЗНАЧЕНИЕ И ЦЕЛИ СОЗДАНИЯ СИСТЕМЫ

2.1. Назначение системы

Разрабатываемое приложение предназначено для коммерческих целей, с задачей повысить эффективность работы предприятия-заказчика.

2.2. Цели создания системы

Целью разработки является повышение эффективности маркетинга предприятия, а также упрощение его основных бизнес-процессов.

3 ТРЕБОВАНИЯ К ПРОГРАММНОМУ ПРОДУКТУ

3.1 Требования к приложению

3.1.1 Требования к структуре и функционированию

В приложении можно выделить следующие функции:

1) Возможность регистрации и авторизации пользователя. После регистрации появится возможность отслеживать личную ежемесячную статистику продаж.

2) Пользователю должны быть предоставлены возможности для упрощённого создания документов с использованием шаблонов.

3) Пользователю должна быть предоставлено право чтения, добавления, изменения и удаления данных о клиентах в БД.

4) Пользователь должен иметь быстрый доступ к актуальным прайс-листам поставщиков.

Все элементы интерфейса должны быть четко различимы и выполнены в одной цветовой гамме для наилучшего восприятия.

3.1.2. Требования к квалификации и численности персонала, режиму его работы

Для обеспечения работы приложения нужно два пользователя. Администратор, заранее обученный работе с программой и обладающий расширенными правами доступа и пользователь, имеющий обычные права.

3.1.4 Требования безопасности

К программе предъявляются следующие требования безопасности:

1) Система должна содержать идентификацию пользователя.

2) Надежное хранение данных;

3) Система должна обладать таким свойством, как предотвращение ввода некорректных данных;

4) Надежная передача данных.

3.1.5 Требования к интерфейсу пользователя

Система должна иметь человеко-машинный интерфейс, удовлетворяющий следующим требованиям:

– взаимодействие системы и пользователя должно осуществляться на русском языке, за исключением системных сообщений, не подлежащих русификации;

– должно быть реализовано отображение на экране только тех возможностей, которые доступны конкретному пользователю в соответствии с его функциональной ролью в системе;

– допустима видимость предоставляемой информации на экране;

– допустимая цветопередача.

3.1.6 Требования к эксплуатации, техническому обслуживанию, ремонту и хранению.

Пользователи обязаны быть проинформированы о правилах использования технических средств и работы с программой и с оборудованием, на котором используется данная программа.

Устройство хранения должно быть защищено от внешних физических воздействий, в качестве переноса и хранения может быть любой диск для хранения данных.

Программные средства администратора системы должны обеспечивать:

1. при выходе технических средств из строя, должна обеспечиваться ее замена без потери функциональной подсистемы;
2. полное или частичное восстановление потерянной информации;
3. протокол действий при возникновении нештатной ситуации.

3.2 Требования к видам обеспечения

3.2.1 Требования к информационному обеспечению и программной документации

Данные, обрабатываемые в приложении, должны храниться в БД на сервере, реализуемой средствами C# и SQL для манипулирования ими.

Состав программной документации, предъявляемой на испытании:

- ГОСТ 19.402-78 – описание программы;
- ГОСТ 19.301-79 – программа и методика испытаний;
- ГОСТ 19.401-78 – тестирование программы.

3.2.2 Требования к лингвистическому обеспечению

Для создания данной программы необходимы знания языков C# и SQL, функционала Microsoft WPF и Microsoft SQL Server.

3.2.3 Требования к программному обеспечению

Для реализации и эксплуатации симулятора пользователь должен иметь установленную операционную систему Windows 8/8.1/10 и ный .NET Framework 4.5.2/4.6/4.6.1/4.6.2/4.7/4.7.1/ 4.7.2.

3.2.4 Требования к техническому обеспечению

Минимальные требования для работы на персональных компьютерах, имеющих следующие минимальные характеристики:

- тактовая частота процессора – 2.0 ГГц;
- ОЗУ - 4 ГБ или более

- на жестком диске при установке используется около 200 Мбайт;

К дополнительным требованиям относятся:

- устройство ввода информации: клавиатура, мышь;
- монитор;

4 СОСТАВ И СОДЕРЖАНИЕ РАБОТ ПО СОЗДАНИЮ СИСТЕМЫ

Этапы, которые необходимо выполнить по созданию приложения:

1 этап – Изучение предметной области, анализ процессов деятельности организации. В конце этого этапа будут разработаны диаграммы внешнего и внутреннего документооборота;

2 этап – Проектирование программного обеспечения с использованием языка UML;

3 этап – Создание базы данных.

4 этап – Разработка программного продукта с использованием языка C# и средств Microsoft WPF.

5 этап – Согласование программной реализации приложения с требованиями заказчика с учетом всех замечаний и пожеланий.

6 этап – Внедрение и сопровождение приложения: установка и настройка программного и аппаратных средств, обучение пользователей работе с системой и приложением, выявление и устранение неполадок.

5 ТРЕБОВАНИЯ К ПРИЕМКЕ-СДАЧЕ ПРОЕКТА

В рамках работ по данному проекту исполнитель разрабатывает приложение, необходимое заказчику.

Приемка готового программного продукта в соответствии со следующим планом:

1 этап – анализ готового проекта;

2 этап – сравнение готового проекта с техническим заданием для определения степени соответствия поставленным задачам и требованиям;

3 этап – внесение коррективов и дополнений в систему по результатам предыдущих этапов;

4 этап – составление списка преимуществ и недостатков разработанного программного продукта.

6 ТРЕБОВАНИЯ К СОСТАВУ И СОДЕРЖАНИЮ РАБОТ ПО ПОДГОТОВКЕ ОБЪЕКТА АВТОМАТИЗАЦИИ К ВВОДУ СИСТЕМЫ В ДЕЙСТВИЕ

Перед вводом в эксплуатацию готового программного продукта исполнитель должен договориться с руководителем организации о временном промежутке, в течение которого он обязан внедрить разработанный программный продукт. Под внедрением понимается комплекс мероприятий, включающий обучение персонала, настройку системы для дальнейшего использования, предоставление им необходимой документации для системы, ознакомление инструктора с его обязанностями.

7 ТРЕБОВАНИЯ К ДОКУМЕНТИРОВАНИЮ

При вводе программы в эксплуатацию пакет сопроводительных документов должен включать:

– техническое задание;

– описание программного продукта;

– руководство пользователя;

8 ПОРЯДОК ПЕРЕНОСА ПРОГРАММНОГО ПРОДУКТА НА ТЕХНИЧЕСКИЕ СРЕДСТВА ЗАКАЗЧИКА

После завершения сдачи-приемки программы, в рамках гарантийной поддержки исполнителем производится однократный перенос разработанного программного обеспечения на аппаратные средства Заказчика.

Подпись Исполнителя _____

ПРИЛОЖЕНИЕ Б

Таблица Б.1 – Угрозы и их характеристики

Наименование угрозы	Вероятность (Y2)	Реализуемость (Y)	Опасность	Актуальность
1	2	3	4	5
Угрозы утечки информации по техническим каналам				
Угрозы утечки акустической (речевой) информации	маловероятно (0)	низкая (0.25)	низкая	неактуальная
Угрозы утечки видовой информации	маловероятно (0)	низкая (0.25)	низкая	неактуальная
Угрозы утечки информации по каналу ПЭМИН	маловероятно (0)	низкая (0.25)	низкая	неактуальная
Сетевые угрозы				
Угрозы "Анализа сетевого трафика" с перехватом передаваемой по сети информации	низкая вероятность (2)	средняя (0.35)	средняя	актуальная
Угрозы выявления паролей	низкая вероятность (2)	средняя (0.35)	средняя	актуальная
Угрозы удаленного запуска приложений	низкая вероятность (2)	средняя (0.35)	средняя	актуальная
Угрозы внедрения по сети вредоносных программ	низкая вероятность (2)	средняя (0.35)	низкая	актуальная
Угрозы из внешних сетей				
Угрозы "Анализа сетевого трафика" с перехватом передаваемой во внешние сети и принимаемой из внешних сетей информации	низкая вероятность(2)	средняя (0.35)	средняя	актуальная
Угрозы сканирования, направленные на выявление типа операционной системы АРМ, открытых портов и служб, открытых соединений и др.	маловероятно (0)	низкая (0.25)	низкая	неактуальная
Угрозы выявления паролей	низкая вероятность (2)	средняя (0.35)	средняя	актуальная
Угрозы получения НСД путем подмены доверенного объекта	маловероятно (0)	низкая (0.25)	низкая	неактуальная

Продолжение таблицы Б.1

1	2	3	4	5
Угрозы типа "Отказ в обслуживании"	низкая вероятность(2)	средняя (0.35)	средняя	актуальная
Угрозы удаленного запуска приложений	маловероятно (0)	низкая (0.25)	низкая	неактуальная
Угрозы внедрения по сети вредоносных программ	средняя вероятность(5)	средняя (0.5)	средняя	актуальная
Угрозы НСД к ПДн непосредственно в ИСПДн				
Угрозы, реализуемые в ходе загрузки операционной системы и направленные на перехват паролей или идентификаторов, модификацию базовой системы ввода/вывода (BIOS), перехват управления загрузкой	маловероятно (0)	низкая (0.25)	средняя	неактуальная
Угрозы внедрения вредоносных программ	средняя вероятность (5)	средняя (0.5)	низкая	неактуальная
Угрозы, реализуемые после загрузки операционной системы и направленные на выполнение несанкционированного доступа с применением стандартных функций (уничтожение, копирование, перемещение, форматирование и т.п.) операционной системы или какой-либо прикладной программы, с применением специально созданных для выполнения НСД программ	маловероятно (0)	низкая (0.25)	средняя	неактуальная