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
И.о. зав. кафедрой
_____ А.В. Бушманов
«07» 07 2020 г.

БАКАЛАВРСКАЯ РАБОТА

на тему: Разработка политики безопасности предприятия

Исполнитель
студент группы 655-об _____ 29.06.2020 _____ Н.Ю. Копылов
(подпись, дата)

Руководитель
доцент, канд. техн. наук _____ 30.06.2020 _____ С.Г. Самохвалова
(подпись, дата)

Консультант
по безопасности
и экологичности
доцент, канд. техн.
наук _____ 29.06.2020 _____ А.Б. Булгаков
(подпись, дата)

Нормоконтроль
доцент, канд.техн.наук _____ О.В. Жилиндина
(подпись, дата)

Благовещенск 2020

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
И.о. зав. кафедрой
_____ А.В. Бушманов
«20» 02 2020 г.

З А Д А Н И Е

К бакалаврской работе студента Копылова Никиты Юрьевича.

1. Тема выпускной работы: Разработка политики безопасности предприятия
(утверждена приказом от 30.04.2020 № 810-уч)

2. Срок сдачи студентом законченной работы 26.06.2020 г.

3. Исходные данные к бакалаврской работе: отчёт по преддипломной практике

4. Содержание бакалаврской работы: описание предметной области, этапы проектирования программного обеспечения, описание разработанного программного обеспечения, руководство пользователя, безопасность и экологичность.

5. Перечень материалов: техническое задание, функциональная структура ИС

6. Консультант по безопасности и экологичности Булгаков Андрей Борисович доцент, канд. техн. наук.

7 Дата выдачи задания: 20 февраля 2020 года

Руководитель бакалаврской работы: Самохвалова Светлана Геннадьевна доцент, канд. техн. наук.

Задание принял к исполнению 20.02.2020: _____ Н.Ю. Копылов

РЕФЕРАТ

Бакалаврская работа содержит 85 с., 64 рисунков, 19 таблиц, 18 источников, 2 приложения

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ, ПОЛИТИКА БЕЗОПАСНОСТИ, ОЦЕНКА РИСКОВ, АВТОМАТИЗИРОВАННАЯ СИСТЕМА, БАЗА ДАННЫХ, ИНФОЛОГИЧЕСКОЕ ПРОЕКТИРОВАНИЕ, ЛОГИЧЕСКОЕ ПРОЕКТИРОВАНИЕ, ФИЗИЧЕСКОЕ ПРОЕКТИРОВАНИЕ

Объект исследования – разработка автоматизированной системы

Цель работы: разработать автоматизированную систему, предназначенную для проведения аудита политики безопасности на соответствие стандарту ГОСТ Р ИСО/МЭК 27002-2012 «Информационная технология (ИТ).

Работа выполнялась в несколько стадий. Первая стадия – описание предметной области исследования. Вторая стадия – выполнение всех этапов проектирования АС. Третья стадия – описание разработанного программного обеспечения, а также составление руководства пользователя. Последняя стадия исследование – рассмотрение вопросов безопасности жизнедеятельности и экологичности.

Результатом выполнения работы является автоматизированная система, позволяющая провести проверку разработанной либо разрабатываемой политики безопасности на соответствие требованиям государственного стандарта ГОСТ Р ИСО/МЭК 27002-2012, а также выполнить анализ существующих рисков безопасности.

СОДЕРЖАНИЕ

НОРМАТИВНЫЕ ССЫЛКИ

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

ГОСТ Р ИСО/МЭК 17799-2005. Информационная технология. Практические правила управления информационной безопасностью

ГОСТ Р ИСО/МЭК 27002-2012. Информационная технология (ИТ). Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности

ГОСТ Р ИСО/МЭК 27005-2010. Информационная технология (ИТ) Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности

ГОСТ Р 53114-2008. Защита информации. Обеспечение информационной безопасности в организации

ГОСТ Р ИСО 6385—2016. Применение эргономических принципов при проектировании производственных систем

СанПиН 2.2.2/2.4.1340-03. Гигиенические требования к персональным электронно-вычислительным машинам и организации работы

СанПиН 2.2.4.3359-16. Санитарно-эпидемиологические требования к физическим факторам на рабочих местах

ОПРЕДЕЛЕНИЯ, ОБОЗНАЧЕНИЯ, СОКРАЩЕНИЯ

АС – автоматизированная система;

БД – база данных;

ИБ – информационная безопасность;

ИТ – информационные технологии;

НФ – нормальная форма;

ВВЕДЕНИЕ

Для большинства организации немаловажным является организация процесса защиты конфиденциальной информации, используемой на предприятии. Причиной этого является то, что утечка подобной информации вследствие использования ненадлежащих мер и средств защиты или полного отказа от них может привести к дестабилизации работы предприятия. При этом недостаточно введения отдельных программных и технических средств. Защита информации на предприятии должна быть комплексной, иметь в качестве основы чётко сформулированную программу защиты, определяющую стратегию организации по обеспечению ИБ. В качестве такой основы обычно выступает политика безопасности, представляющая собой документ, определяющий подход организации к обеспечению безопасности своих информационных ресурсов.

Весьма важным является вопрос соответствия разработанной политики безопасности определённому стандарту. Существует большое количество международных, межгосударственных, национальных стандартов по защите информации. В качестве одного из национальных стандартов РФ можно выделить ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности. Данный стандарт идентичен международному стандарту ИСО/МЭК 27002:2005 и является заменой ГОСТ Р ИСО/МЭК 17799-2005. Настоящий национальный стандарт предлагает рекомендации и основные принципы введения, реализации, поддержки и улучшения менеджмента информационной безопасности в организации.

В рамках данной работы будет разработано программное обеспечение для осуществления проверки политики информационной безопасности на соответствие требованиям стандарта ГОСТ Р ИСО/МЭК 27002-2012.

1 ОПИСАНИЕ ПРЕДМЕТНОЙ ОБЛАСТИ

Объект разработки представляет собой программное обеспечение, предназначенное для проведения аудита политики безопасности на соответствие стандарту ГОСТ Р ИСО/МЭК 27002-2012 «Информационная технология (ИТ). Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности».

В данной главе будут рассмотрены такие понятия, как информационная безопасность, оценка рисков, политика безопасности.

1.1 Информационная безопасность

1.1.1 Основные понятия

Информация – это некоторые сведения, воспринимаемые и обрабатываемые человеком или специальными техническими устройствами

Для любой организации информация – это некий актив, который, как и другие активы организации, имеет ценность и, следовательно, должен быть защищен надлежащим образом, что важно для среды бизнеса.

Информационная безопасность – это защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений.

Информационная безопасность включает в себя защиту конфиденциальности, целостности и доступности информации.

Конфиденциальность – это свойство информации, состоящее в том, что она не может быть доступна кому-либо вне чётко определенного круга лица.

Целостность – это свойство информации, которое характеризует ее устойчивость к случайному или преднамеренному повреждению, или несанкционированному изменению.

Доступность - свойство системы, заключающееся в возможности обеспечения своевременного беспрепятственного доступа правомочных (авторизованных) субъектов к интересующей их информации или осуществления своевременного информационного обмена между ними.

Защита информации может быть определена как деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

Защита информации осуществляется с использованием способов и средств защиты. Способ защиты информации включает в себя порядок и правила применения определенных принципов и средств защиты информации.

Средство защиты информации — это техническое, программное, программно-техническое средство, вещество и (или) материал, предназначенные или используемые для защиты информации.

Таким образом, информационная безопасность достигается путем реализации соответствующего комплекса мер и средств контроля и управления, которые могут быть представлены политиками, процессами, процедурами, организационными структурами, а также функциями программных и аппаратных средств.

1.1.2 Определение требований к информационной безопасности

Любой организацией должны быть определены свои требования к информационной безопасности. Существуют три основных источника требований безопасности.

Первый источник определяется путём проведения оценки рисков организации с учётом общей стратегии и целей бизнеса организации. В результате оценки рисков осуществляется идентификация угроз активам организации, определение уязвимости и вероятности возникновения угроз, а также оценка возможных последствий.

Второй источник - правовые, законодательные, нормативные и договорные требования, которым должны удовлетворять организация, ее торговые партнеры, подрядчики и поставщики услуг, а также их социокультурная среда.

Третий источник представляет собой определенный набор разработанных организацией для поддержки своей деятельности принципов, а также целей и требований бизнеса для обработки информации.

1.2 Оценка рисков

1.2.1 Основные понятия

Основная цель оценки рисков – идентификация рисков, определение их количества и приоритетов. Оценка рисков должна иметь систематический характер и включать в себя анализ рисков и оценивание рисков.

Анализ рисков предполагает выполнение процедур по выявлению факторов рисков и оценку их значимости. Можно выделить два основных вида анализа рисков: качественный и количественный. Качественный анализ направлен на выявление(идентификацию) различных видов риска, их факторов, возможной области возникновения и т.д. Цель количественного анализа – численно определить размеры отдельных рисков и риска предприятия в целом.

После проведения анализа рисков необходимо осуществить оценивание рисков, которое представляет собой сравнение количественно оцененных рисков с данными критериями рисков для определения значимости рисков.

Постоянное изменение и дополнение требований к информационной безопасности предприятия приводит к необходимости периодического проведения оценки рисков с целью учёта произведенных изменений.

Эффективность проведения оценки рисков информационной безопасности будет обеспечиваться только в случае, если чётко определена область применения данной оценки, а также, в случае необходимости, выявлена взаимосвязь данной оценки с оценками рисков в других областях.

В качестве области применения может выступать организация в целом, её подразделения, отдельная информационная система, определенные компоненты системы, или услуги.

ГОСТ Р ИСО/МЭК 27005-2010 «Информационная технология (ИТ)». Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности» определяет различные подходы к оценкам риска ИБ, выделяя два основных метода оценок риска: высокоуровневую и детальную.

1.2.2 Высокоуровневая оценка рисков

Высокоуровневая оценка позволяет определить текущие приоритеты и, на основании этого, построить хронологию действий, которые необходимо произвести в ходе оценки рисков. Например, в некоторых случаях не всегда возможна одновременная реализация всех мер и средств контроля и управления, поэтому в данной ситуации целесообразным будет рассмотреть вначале только наиболее критичные риски. В других случаях начинать детальную оценку всех рисков может быть преждевременным, поэтому сначала можно провести высокоуровневую оценку последствий, а не систематический анализ угроз, уязвимостей, активов и последствий.

Часто оценка риска проводится за две или более итерации. На первом шаге обычно осуществляется именно высокоуровневая оценка, т.к. она позволяет идентифицировать потенциально высокие риски, на основании которых будет произведены дальнейшие оценки.

Таким образом, риски, представленные в высокоуровневой оценке риска, часто носят более общий характер, чем конкретно идентифицированные риски.

Достоинства высокоуровневой оценки риска:

- включение первоначального простого подхода, вероятно, необходимо для одобрения программы оценки риска;

- должно быть возможным создание стратегической картины программы обеспечения безопасности организации, т.е. она будет действовать как хорошая помощь в планировании;

- ресурсы и денежные средства могут быть применены там, где они наиболее полезны, и системы, вероятно, больше всего нуждающиеся в защите, будут рассмотрены первыми.

1.2.3 Детальная оценка рисков

Детальная оценка рисков предполагает тщательное определение и установление ценности активов, оценку угроз этим активам и оценку уязвимостей. Результаты этой деятельности используются для оценки рисков, а затем для определения способа обработки риска.

Данный подход целесообразнее использовать для ИС с высоким уровнем риска, т.к. проведение детальной оценки является достаточно трудоёмким процессов, занимающим значительное время и требующим определённых знаний и умений.

Окончательным этапом детальной оценки риска ИБ является оценка общих рисков, находящаяся в фокусе данного приложения.

Последствия могут оцениваться несколькими методами, включая количественные, например, денежные, и качественные меры (с использованием таких определений, как "умеренные" или "серьезные") или их комбинации. Для оценки вероятности возникновения угрозы должны быть установлены временные рамки, в которых актив будет обладать ценностью или нуждаться в защите.

В данном методе оценки рисков могут использоваться таблицы, содержащие заранее определённые экспериментально значения ценности активов, уровня угроз и уязвимостей.

1.3. Политика безопасности

1.3.1 Основные понятия. Определение состава политики безопасности

Политика безопасности – это совокупность законов, правил и норм поведения, которая определяет средства и методы обработки, защиты и распространения информации в организации.

Любая политика безопасности должна включать основные цели и задачи организации режима информационной безопасности, содержать описание области действия, а также определять ответственных лиц.

Для большинства организаций наличие чётко оформленной политики безопасности является весьма важным условием нормального функционирования.

Важность эта обусловлена главным образом тем, что политика безопасности отражает взгляды руководства организации на защиту информации, используемой на предприятии, от определённых угроз, а также определяет основные технологии обеспечения безопасности информационных ресурсов организации.

Политика безопасности обычно состоит из двух частей: общих принципов и конкретных правил работы с информационными ресурсами и, в частности, с базами данных для различных категорий пользователей. Необходимо учитывать, что политика безопасности является некоторым компромиссом между желаемым уровнем защищенности ресурсов информационной системы, удобством работы с системой и затратами средств, выделяемых на ее эксплуатацию.

Политика безопасности должна быть оформлена документально на нескольких уровнях управления. На уровне управляющего высшего звена руководства должен быть подготовлен и утвержден документ, в котором определены цели политики безопасности, структура и перечень решаемых задач и ответственные за реализацию политики. Основной документ должен быть детализирован администраторами безопасности информационных систем (управляющими среднего звена) с учетом принципов деятельности организации, соотношения важности целей, и наличия ресурсов. Детальные решения должны включать ясные определения методов защиты технических и информационных ресурсов, а также инструкции, определяющие поведение сотрудников в конкретных ситуациях.

Согласно ГОСТ Р 53114-2008 «Защита информации. Обеспечение информационной безопасности в организации.» политика информационной безопасности организации должна содержать следующие сведения:

- предмет, основные цели и задачи политики безопасности;
- условия применения политики безопасности и возможные ограничения;
- описание позиции руководства организации в отношении выполнения политики безопасности и организации режима информационной безопасности организации в целом;

- права и обязанности, а также степень ответственности сотрудников за выполнение политики безопасности организации;

- порядок действия в чрезвычайных ситуациях в случае нарушения политики безопасности.

В разделе «Предмет, основные цели и задачи политики безопасности» должны быть сформулированы основные цели и причины разработки политики, а также должна быть описана область ее применения. Кроме того, в данном разделе необходимо чётко сформулировать и описать задачи, решаемые с использованием информационных систем, на которые распространяются положения данной политики.

Раздел «Условия применения политики безопасности и возможные ограничения» должен содержать описание порядка доступа к данным ИС, а также сведения об ограничениях или технологических цепочках, применяемые при реализации политики безопасности

В разделе «Описание позиции руководства организации» необходимо описать основные информационные ресурсы, используемые в организации, определить перечень лиц и процессов, имеющих доступ к данным ресурсам, а также порядок получения доступа к ним.

В разделе «Права и обязанности» должны быть определены ответственные за соблюдение положений политики должностные лица, а также их обязанности в отношении разработки и внедрения различных элементов политики.

1.3.2. Актуальность разработки политик безопасности для отечественных компаний и организаций

Необходимость формирования механизмов планирования и управления информационной безопасности обуславливают достаточно высокую актуальность разработки политик информационной безопасности для отечественных компаний и организаций. Политики ИБ позволяют решать задачи, непосредственно связанные с процессом деятельности предприятия. Среди таких задач можно выделить:

- минимизация рисков бизнеса путем защиты своих интересов в информационной сфере;

- обеспечение безопасного, доверенного и адекватного управления предприятием;

- планирование и поддержка непрерывности бизнеса;

- повышение качества деятельности по обеспечению информационной безопасности;

- снижение издержек и повышение эффективности инвестиций в информационную безопасность;

- повышение уровня доверия к компании со стороны акционеров, потенциальных инвесторов, деловых партнеров, профессиональных участников рынка ценных бумаг, уполномоченных государственных органов и других заинтересованных сторон.

1.4 ГОСТ Р ИСО/МЭК 27002-2012

Стандарт ГОСТ Р ИСО/МЭК 27002-2012 утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 24 сентября 2012 г. N 423-ст. Данный стандарт заменяет ГОСТ Р ИСО/МЭК 17799-2005 и является идентичным международному стандарту ИСО/МЭК 27002:2005* "Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности".

Настоящий национальный стандарт предлагает рекомендации и основные принципы введения, реализации, поддержки и улучшения менеджмента информационной безопасности в организации. Цели, изложенные в данном национальном стандарте, обеспечивают полное руководство по общепринятым целям менеджмента информационной безопасности.

Реализация целей управления, а также мер и средств контроля и управления настоящего национального стандарта направлена на удовлетворение требований, определенных оценкой рисков. Настоящий национальный стандарт мо-

жет служить практическим руководством по разработке стандартов безопасности организации, для эффективной практики менеджмента безопасности организаций и способствует укреплению доверия в отношениях между организациями.

Стандарт состоит из одиннадцати разделов, содержащих описание мер и средств контроля и управления безопасности и включающих 39 основных категорий безопасности. Названия данных разделов перечислены ниже:

- политика безопасности;
- организационные аспекты информационной безопасности;
- менеджмент активов;
- безопасность, связанная с персоналом;
- физическая защита и защита от воздействия окружающей среды;
- менеджмент коммуникаций и работ;
- управление доступом;
- приобретение, разработка и эксплуатация информационных систем;
- менеджмент инцидентов информационной безопасности;
- менеджмент непрерывности бизнеса;
- соответствие.

2 ЭТАПЫ ПРОЕКТИРОВАНИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

2.1 Обоснование необходимости создания системы

Разрабатываемое программное обеспечение предназначено для осуществления проверки политики безопасности на соответствие требованиям ГОСТ Р ИСО/МЭК 27002-2012.

Необходимость разработки обусловлена потребностью в создании удобного и интуитивно понятного средства, которое позволило бы аудитору провести проверку существующей либо готовящейся политики безопасности на соответствие определённому стандарту безопасности.

Проведение аудита безопасности позволяет выявить существующие угрозы безопасности бизнес-процессов организации, а также выработать рекомендации по повышению уровня защищённости информационных ресурсов организации.

Проверка соответствия политики безопасности определённому государственному стандарту позволяет оценить, насколько утверждённые или готовящиеся к утверждению средства и меры по обеспечению безопасности отвечают требованиям, утверждёнными именно на государственном уровне. Данные требования являются определённой базой для оценки уровня защищённости организации, поэтому весьма важно учитывать их при организации системы защиты информации на предприятии.

Результаты проверки могут быть использованы для разработки комплексного плана внесения изменений в систему управления информационной безопасностью, как для повышения реального уровня защищенности, так и для непосредственного соответствия стандарту.

Также необходимость разработки обусловлена тем, что существующие программные средства проверки политики безопасности, такие Cobra и КОНДОР+, в настоящее время труднодоступны. В случае же, если доступ к данному ПО всё же будет получен, запуск этих программ на современных ОС может быть затруднителен либо невозможен вообще.

Таким образом, можно выделить следующие цели разработки:

- упрощение проведения аудита информационной безопасности;
- повышение эффективности анализа рисков;

2.2 Обоснование выбора среды разработки

В качестве языка программирования был выбран язык C#. Данный язык использует объектно-ориентированный подход, который позволяет представить программу в виде совокупности объектов, являющихся экземплярами того или иного класса, организовать взаимодействие между классами, определив наследование и т.д. Всё это позволяет существенно облегчить разработку путём повышения адаптивности разрабатываемой системы. Также можно отметить, что в C# имеется достаточное количество готовых синтаксических конструкций, использование которых может облегчить процесс написания кода.

Для разработки был выбран интерфейс программирования приложений Windows Forms. Данный интерфейс даёт возможность получить доступ к элементам интерфейса Microsoft Windows и использовать их для создания графического пользовательского интерфейса приложения (GUI).

В качестве среды разработки будет использоваться Microsoft Visual Studio. Данная среда разработки поддерживает множество языков программирования и имеет набор всех средств, необходимых для разработки приложения.

В качестве СУБД была выбрана MySQL. Данная СУБД является достаточной распространённой, имеет открытый код, а также обладает достаточным количеством преимуществ. Во-первых, MySQL проста в использовании и позволяет облегчить работу с БД. Во-вторых, данная СУБД имеет весьма широкий набор инструментов, необходимых для выполнения тех или иных задач. В-третьих, стоит отметить её масштабируемость, что позволяет использовать MySQL для работы как с малыми, так и с большими объёмами данных. Также MySQL обеспечивает достаточно высокую скорость работы за счёт упрощения некоторых используемых в ней стандартов.

Таким образом, MySQL является достаточно универсальной СУБД, имеющей большое количество достоинств. Поэтому именно она была выбрана для проекта.

В качестве локального сервера для базы данных был выбран MAMP. MAMP является бесплатным и достаточно простым в установке приложением. При этом MAMP не ставит под угрозу уже существующую установку Apache в системе. Установка компонентов MAMP происходит без запуска скриптов и изменения конфигурационных файлов. Удаление приложения происходит простым удалением его папки. При этом после удаления не остаётся каких-либо остаточных файлов, т.е. MAMP ничего не изменяет в системе.

Также выбор MAMP обоснован тем, что он поддерживает СУБД MySQL, которая будет использоваться при разработке. При этом MAMP предоставляет возможность использовать PhpMyAdmin – веб-приложение для осуществления администрирования сервера MySQl, которое и будет использована для создания и заполнения БД. Кроме MySQL, данное приложение поддерживает следующие компоненты: Apache, Nginx, PHP, Caches, MAMP Cloud.

2.3 Характеристика функциональных подсистем проектируемой ИС

Функциональные подсистемы представляют собой части системы, выделяемые по определенному признаку и отвечающие конкретным целям и задачам. Функциональная модель автоматизированной системы, построенная с использованием методологии IDEF0, представлена в приложении А.

Учитывая задачи, на решение которых будет направлена разрабатываемая система, можно выделить следующие функциональные подсистемы:

1) Подсистема авторизации;
2) Подсистема проведения аудита безопасности;
3) Подсистема редактирования и добавления требований
4) Подсистема представления результатов аудита;
5) Подсистема анализа рисков;
6) Подсистема формирования отчётов;
7) Подсистема управления списком пользователей

Подсистема авторизации получает на вход данные для входа в систему (логин и пароль) и выполняет аутентификацию и авторизацию пользователя

Подсистема проведения аудита безопасности получает список вопросов, предназначенных для проверки соответствия требованиям, а также данные аудитора. Основное назначение данной подсистемы – проведение проверки соответствия требованиям стандарта и, соответственно, добавление результатов проверки в БД, а также предоставление их подсистеме анализа рисков.

Подсистема редактирования и добавления требований предназначена, соответственно, для добавления новых и редактирования существующих требований, а также связанных с ними разделов тестирования и вопросов. Данная подсистема, в случае добавления новых записей, получает список требований извне от пользователя и из базы данных, в случае редактирования. Все проведённые изменения она также добавляет в базу данных.

Подсистема представления результатов аудита предназначена для вывода результатов проведённых аудитов. Данная подсистема предоставляет возможность просмотра общей информации обо всех проведённых аудитах, а также подробной информации с указанием всех выполненных и невыполненных рисков, данных аудитора и т.д. для выбранного аудита.

Подсистема анализа рисков получает результаты проведённой проверки от подсистемы проведения аудита безопасности и осуществляет анализ рисков на основе весовых коэффициентов, установленных у каждого требования.

Подсистема формирования отчётов получает результаты ранее проведённых аудитов из БД. Данная подсистема предназначена для формирования предварительно настроенных отчётов в формате .xls, содержащих сведения о результатах проведённых аудитов.

Подсистема управления списком пользователей получает список пользователей из БД. Данная подсистема предназначена для осуществления добавления новых пользователей системы, редактирования логинов и паролей старых пользователей, а также их удаления.

2.4 Характеристика обеспечивающих подсистем проектируемой ИС

2.4.1 Техническое обеспечение

Техническое обеспечение включает в себя комплекс технических средств, используемых для работы автоматизированной системы.

Минимальные технические характеристики ПК клиента:

- тактовая частота процессора не ниже 1,8 ГГц;
- 2 ГБ ОЗУ;
- 800 Мб на жёстком диске;

Минимальные технические характеристики ПК сервера:

- тактовая частота процессора не ниже 3 ГГц;
- 4 ГБ ОЗУ;
- жёсткий диск объёмом 500 Гб;

2.4.2 Программное обеспечение

Программное обеспечение включает комплекс программ, необходимых для нормальной работы разрабатываемой системы, а также обеспечивающих функционирование комплекса технических средств.

На сервере может быть установлена одна из перечисленных ОС семейства Windows: Windows 7, Windows 8.1, Windows 10. В качестве локальной серверной среды должна быть установлена MAMP.

2.4.3 Лингвистическое обеспечение

Лингвистическое обеспечение включает совокупность научно-технических терминов и других языковых средств, используемых в информационных системах, а также правил формализации естественного языка.

В случае разрабатываемой системы лингвистическое обеспечение включает языки C# и SQL.

2.5 Проектирование базы данных

2.5.1 Инфологическое проектирование

Первый этап инфологического проектирования – формирование набора сущностей. Ниже приведен список сущностей с их краткой характеристикой.

1. Сущность «Раздел» хранит данные о всех разделах теста с указанием их наименований.

2. Сущность «Требование» содержит данные о всех требованиях, на соответствие которым будет проходит проверка.

3. Сущность «Вопрос» содержит информацию о вопросах теста, ответы на которые будут определять соответствие или несоответствие тестируемой политики безопасности требованиям.

4. Сущность «Ответ» хранит данные о всех доступных ответах на каждый вопрос с указанием, является ли данный ответ верным.

5. Сущность «Аудит» содержит данные о проведённых аудитах.

6. Сущность «Результаты аудита» хранит данные о результатах проведённых аудитов.

7. Сущность «Аудитор» содержит информацию об аудиторах, проводивших тестирование.

8. Сущность «Данные для входа» содержит данные, необходимые пользователю для входа в систему.

Второй этап – формирование спецификации атрибутов каждой сущности. В таблицах 1-8 представлены спецификации атрибутов для каждой сущности

Таблица 1 - Спецификация атрибутов сущности «Раздел»

Название атрибута	Описание атрибута	Единица измерения	Диапазон значений	Пример атрибута
Код раздела	Число, однозначно определяющее каждый раздел	-	>0	1
Название раздела	Название раздела тестирования	-	-	Политика безопасности
Описание раздела	Описание раздела тестирования	-	-	Содержит все необходимые требования, предъявляемые к ПБ

Таблица 2 - Спецификация атрибутов сущности «Требование»

Название атрибута	Описание атрибута	Единица измерения	Диапазон значений	Пример атрибута
Код требования	Число, однозначно определяющее каждое требование	-	>0	1
Код раздела	Число, однозначно определяющее каждый раздел	-	>0	3
Текст требования	Содержимое требования	-	-	Высшее руководство должно обеспечивать ресурсы, необходимые для ИБ
Весовой коэффициент	Весовой коэффициент, используемый для расчёта рисков	-	-	50

Таблица 3 - Спецификация атрибутов сущности «Вопрос»

Название атрибута	Описание атрибута	Единица измерения	Диапазон значений	Пример атрибута
Код вопроса	Число, однозначно определяющее каждый вопрос	-	>0	1
Код требования	Число, однозначно определяющее каждое требование	-	>0	2
Текст вопроса	Содержимое вопроса	-	-	Утверждена ли политика информационной безопасности организации высшим руководством?

Таблица 4 - Спецификация атрибутов сущности «Ответ»

Название атрибута	Описание атрибута	Единица измерения	Диапазон значений	Пример атрибута
Код ответа	Число, однозначно определяющее каждый ответ	-	>0	1
Код вопроса	Число, однозначно определяющее каждый вопрос	-	>0	2
Текст ответа	Содержимое ответа	-	-	Да
Является верным	Указание, является ли данный ответ правильным	-	-	True

Таблица 5 - Спецификация атрибутов сущности «Аудит»

Название атрибута	Описание атрибута	Единица измерения	Диапазон значений	Пример атрибута
Код аудита	Число, однозначно определяющее каждый аудит	-	>0	1
Код аудитора	Число, однозначно определяющее каждого аудитора	-	>0	2
Дата проведения	Дата проведения аудита	-	-	12.04.2020
Значение риска, %	Вычисленное значение риска	-	>=0	56,7

Таблица 6 - Спецификация атрибутов сущности «Результаты аудита»

Название атрибута	Описание атрибута	Единица измерения	Диапазон значений	Пример атрибута
1	2	3	4	5
Код аудита	Число, однозначно определяющее каждый аудит	-	>0	1
Код ответа	Число, однозначно определяющее каждый ответ	-	>0	2
Код вопроса	Число, однозначно определяющее каждый вопрос	-	>0	3

Продолжение таблицы 6

1	2	3	4	5
Комментарий аудитора	Комментарий аудитора к выбранному ответу	-	-	Необходимо пересмотреть данное требование

Таблица 7 - Спецификация атрибутов сущности «Аудитор»

Название атрибута	Описание атрибута	Единица измерения	Диапазон значений	Пример атрибута
Код аудитора	Число, однозначно определяющее каждый аудит	-	>0	1
Фамилия	Фамилия аудитора	-	-	Иванов
Имя	Имя аудитора	-	-	Андрей
Отчество	Отчество аудитора	-	-	Петрович
Должность	Должность аудитора	-	-	Специалист по ИБ

Таблица 8 - Спецификация атрибутов сущности «Данные для входа»

Название атрибута	Описание атрибута	Единица измерения	Диапазон значений	Пример атрибута
1	2	3	4	5
Код аудитора	Число, однозначно определяющее каждого аудитора	-	>0	1
Логин	Уникальное имя учётной записи пользователя	-	>0	Admin
Пароль (Хеш)	Значение пароля, преобразованное с помощью хеш-функции SHA512	-	-	f709d23ad6a204d9efc283caea0da87746f313ce97b9beb6546461d1029a7ba46d437bfaca35b8acfd3b9d0c5dd5cb65c85a5cc804fdbc7e1f1e65930848391

Продолжение таблицы 8

1	2	3	4	5
Соль	Случайная строка символов, передаваемая хеш-функции вместе с паролем	-	-	W2HSJak-nmxолфоыв
Права администратора	Указание, обладает ли пользователь правами администратора	-	-	True

Четвертый этап – обоснование установления связей. На рисунках представлено установление связей между сущностями.

Рисунок 1 – Связь «Раздел-Требование»

Рисунок 2 – Связь «Вопрос-Требование»

Рисунок 3 – Связь «Вопрос-Ответ»

Рисунок 4 – Связь «Аудит-Результаты аудита»

Рисунок 5 – Связь «Вопрос-Результаты аудита»

Рисунок 6 – Связь «Ответ-Результаты аудита»

Рисунок 7 – Связь «Аудитор-Аудит»

Рисунок 8 – «Аудитор-Данные для входа»

2.5.2 Логическое проектирование

Логическое проектирование баз данных осуществляется в два этапа.

Первый этап - отображение полученной концептуально-инфологических-кой модели на реляционную модель путем совместного представления в ее отношениях ключевых элементов взаимосвязанных записей. На рисунках 8-21 рассмотрены связи между всеми сущностями.

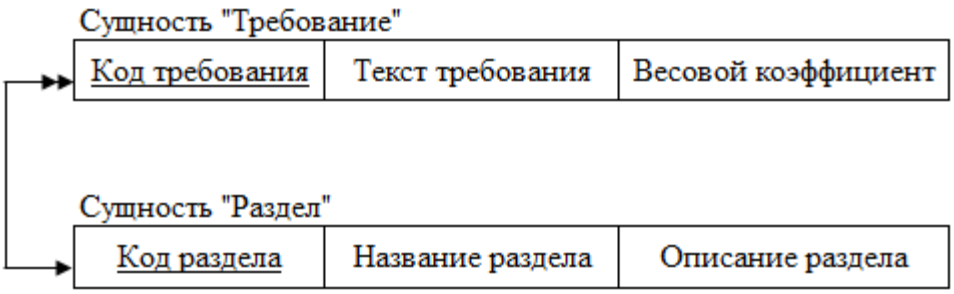

Рисунок 8 - Связь «Раздел-Требование»

Сущность «Раздел» - исходная (родительская), т.к. от нее исходит простая связь. Сущность «Требование» - порожденная (дочерняя). Следовательно, ключ «Код раздела» исходной сущности добавляем в порожденную (дочернюю) сущность, что показано на рисунке 9.

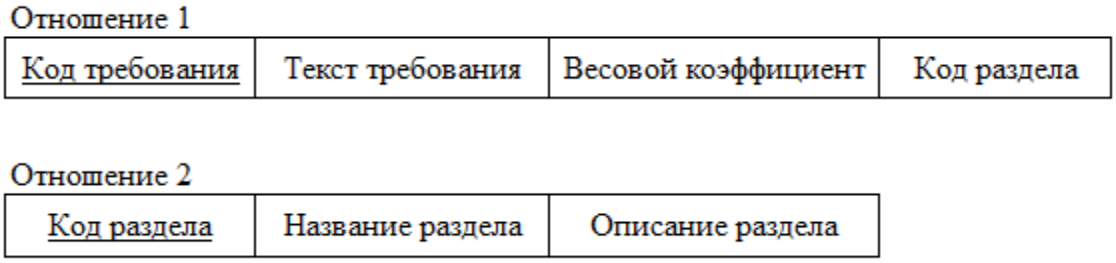

Рисунок 9 – Результат анализа связи «Раздел-Требование»

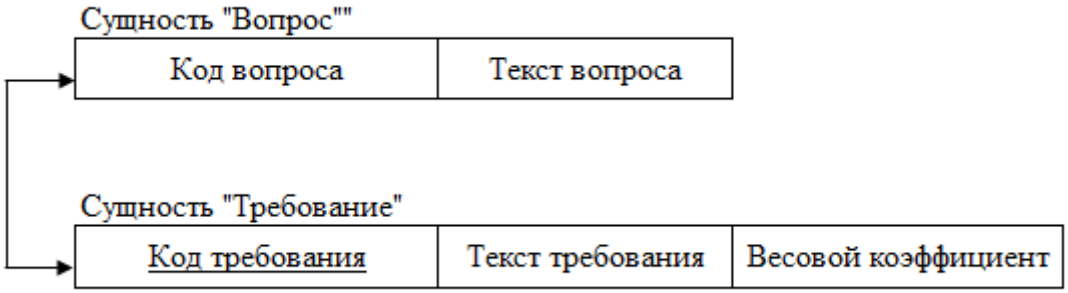

Рисунок 10 - Связь «Требование-Вопрос»

Сущность «Требование» - исходная (родительская), т.к. от нее исходит простая связь. Сущность «Вопрос» - порождённая (дочерняя). Ключ «Код требования» исходной сущности добавляем в дочернюю сущность.

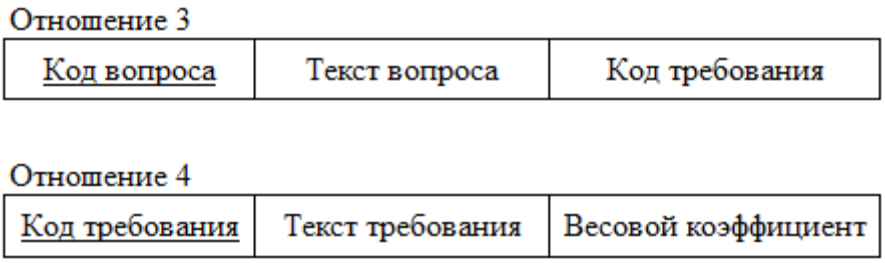

Рисунок 11 - Результат анализа связи «Требование-Вопрос»

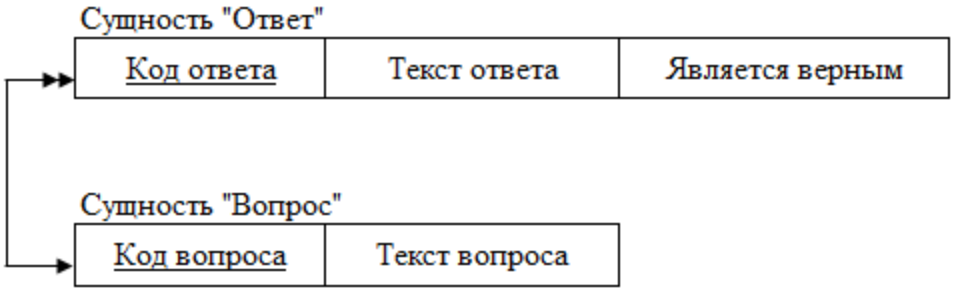

Рисунок 12 - Связь «Вопрос-Ответ»

Сущность «Вопрос» - исходная (родительская), т.к. от нее исходит простая связь. Сущность «Ответ» будет порожденной (дочерней). Следовательно, ключ «Код вопроса» исходной сущности добавляем в порожденную (дочернюю) сущность, что показано на рисунке 13.

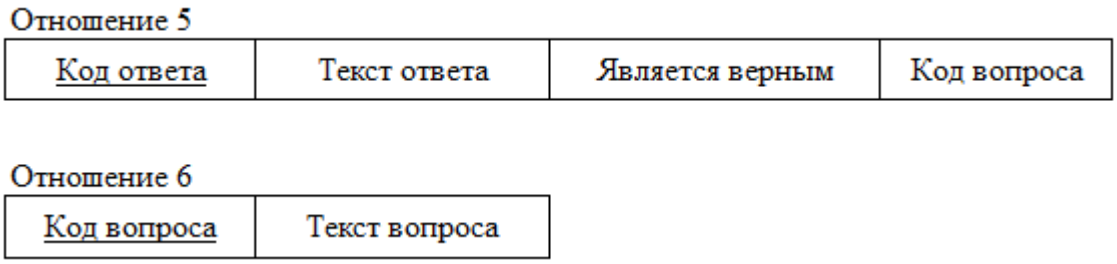

Рисунок 13 - Результат анализа связи «Вопрос-Ответ»

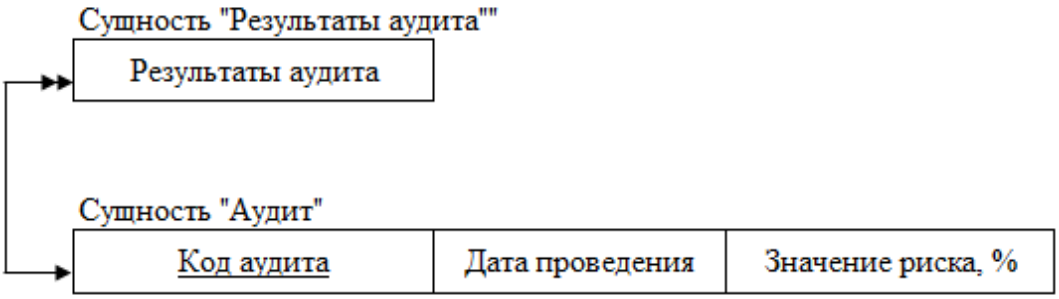

Рисунок 14 - Связь «Аудит-Результаты аудита»

Сущность «Аудит» является исходной (родительской), т.к. от нее исходит простая связь. Сущность «Результаты аудита» будет порожденной (дочерней). Следовательно, ключ «Код аудита» исходной сущности добавляем в порожденную (дочернюю) сущность, что показано на рисунке 15.

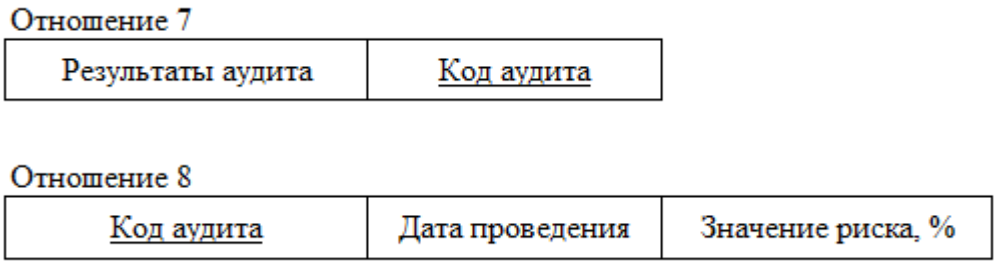

Рисунок 15 - Результат анализа связи «Аудит-Результаты аудита»

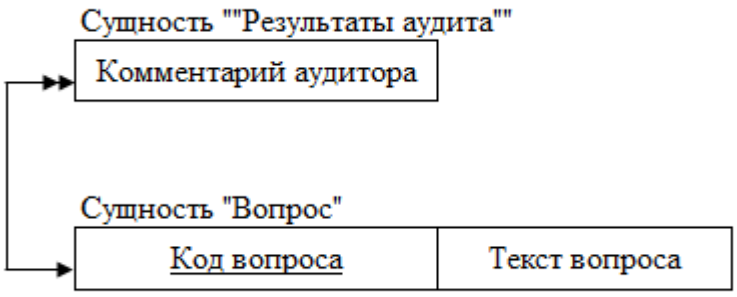

Рисунок 16 - Связь «Вопрос-Результаты аудита»

Сущность «Вопрос» является исходной (родительской), т.к. от нее исходит простая связь. Сущность «Результаты аудита» будет порожденной (дочерней).

Следовательно, ключ «Код вопроса» исходной сущности добавляем в порожденную (дочернюю) сущность, что показано на рисунке 17.

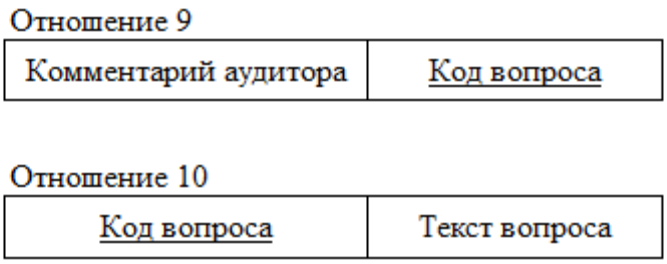

Рисунок 17 - Результат анализа связи «Вопрос-Результаты аудита»

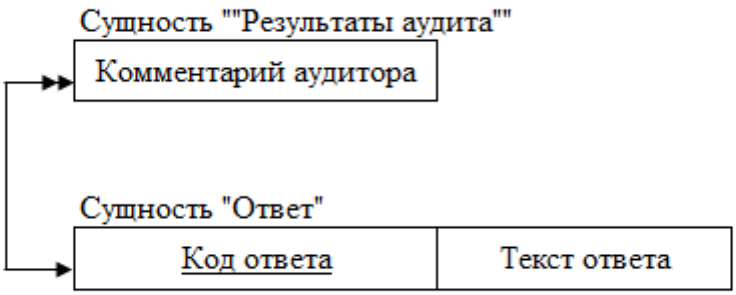

Рисунок 18 - Связь «Ответ-Результаты аудита»

Сущность «Ответ» является исходной (родительской), т.к. от нее исходит простая связь. Сущность «Результаты аудита» будет порожденной (дочерней). Следовательно, ключ «Код ответа» исходной сущности добавляем в порожденную (дочернюю) сущность, что показано на рисунке 19.

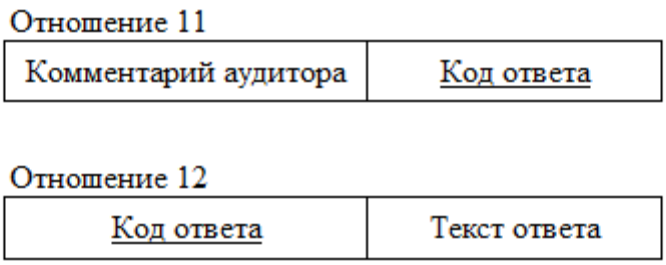

Рисунок 19 - Результат анализа связи «Ответ-Результаты аудита»

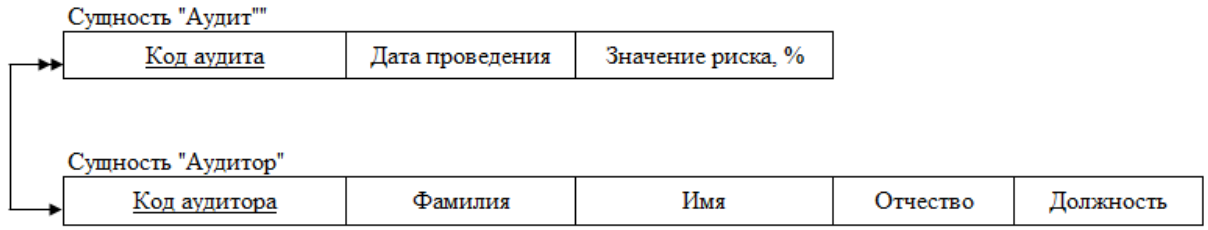

Рисунок 20 - Связь «Аудитор-Аудит»

Сущность «Аудитор» является исходной (родительской), т.к. от нее исходит простая связь. Сущность «Аудит» будет порожденной (дочерней). Следовательно, ключ «Код аудитора» исходной сущности добавляем в порожденную (дочернюю) сущность, что показано на рисунке 21.

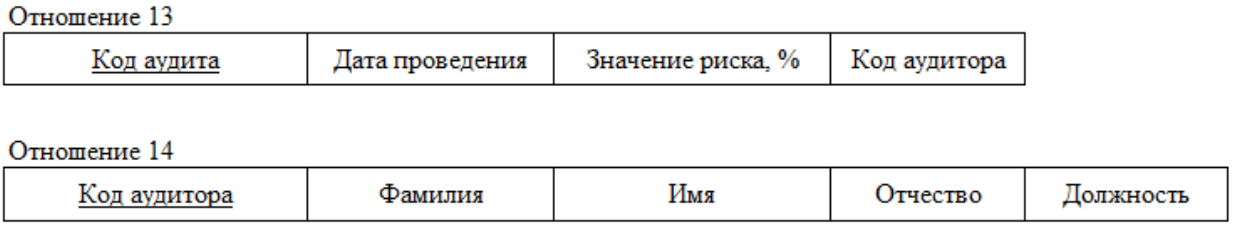

Рисунок 21 - Результат анализа связи «Аудитор-Аудит»

Рисунок 22 - Рисунок 20 - Связь «Аудитор-Данные для входа»

Сущность «Аудитор» является исходной (родительской), т.к. от нее исходит простая связь. Сущность «Данные для входа» будет порожденной (дочерней). Следовательно, ключ «Код аудитора» исходной сущности добавляем в порожденную (дочернюю) сущность, что показано на рисунке 23.

Отношение 15

Логин	Пароль (Хеш)	Соль	Права администратора	Код аудитора

Отношение 16

Код аудитора	Фамилия	Имя	Отчество	Должность

Рисунок 23 - Результат анализа связи «Аудитор-Данные для входа»

Второй этап логического проектирования – нормализация отношений, который предусматривает рассмотрение полученных отношений на соответствие 1НФ, 2НФ, 3НФ.

На рисунках 24 – 31 представлены функциональные зависимости всех отношений.

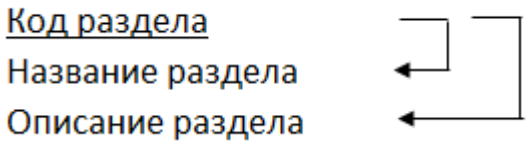

Рисунок 24 - Функциональная зависимость отношения 1

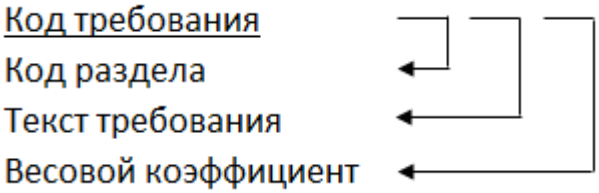

Рисунок 25 - Функциональная зависимость отношения 2

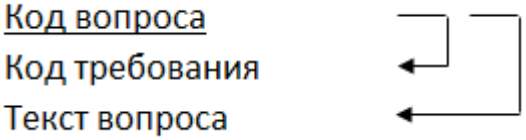

Рисунок 26 - Функциональная зависимость отношения 3

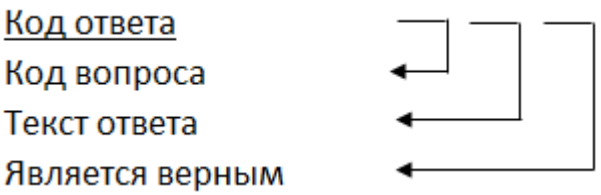

Рисунок 27 - Функциональная зависимость отношения 4

Рисунок 28 - Функциональная зависимость отношения 5

Рисунок 29 - Функциональная зависимость отношения 6

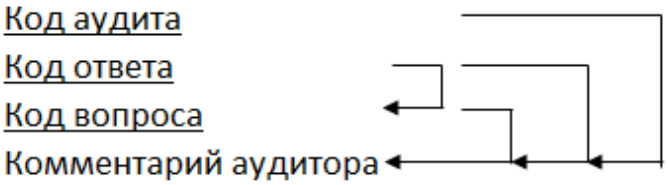

Рисунок 30 - Функциональная зависимость отношения 7

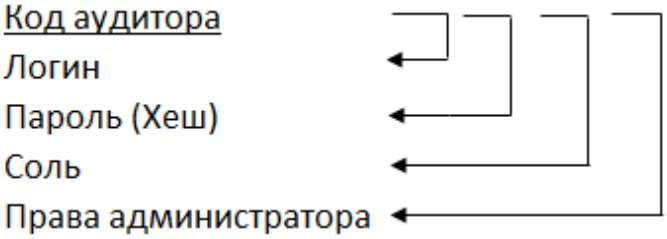

Рисунок 31 – Функциональная зависимость отношения 8

Представленные на рисунках 24 – 31 отношения находятся в первой нормальной форме, так как значения всех атрибутов являются неделимыми или атомарными.

Исследуемые отношения также находятся во второй нормальной форме, поскольку они соответствуют первой нормальной форме и все не ключевые атрибуты функционально полно зависят от первичного ключа.

Также данные отношения находятся в третьей нормальной форме, так как они соответствуют второй нормальной форме и все атрибуты, которые не являются ключевыми, не имеют транзитивной зависимости от ключевых атрибутов.

Результатом логического проектирования БД является логическая модель БД в нотации IDEF1X, представленная на рисунке 32.

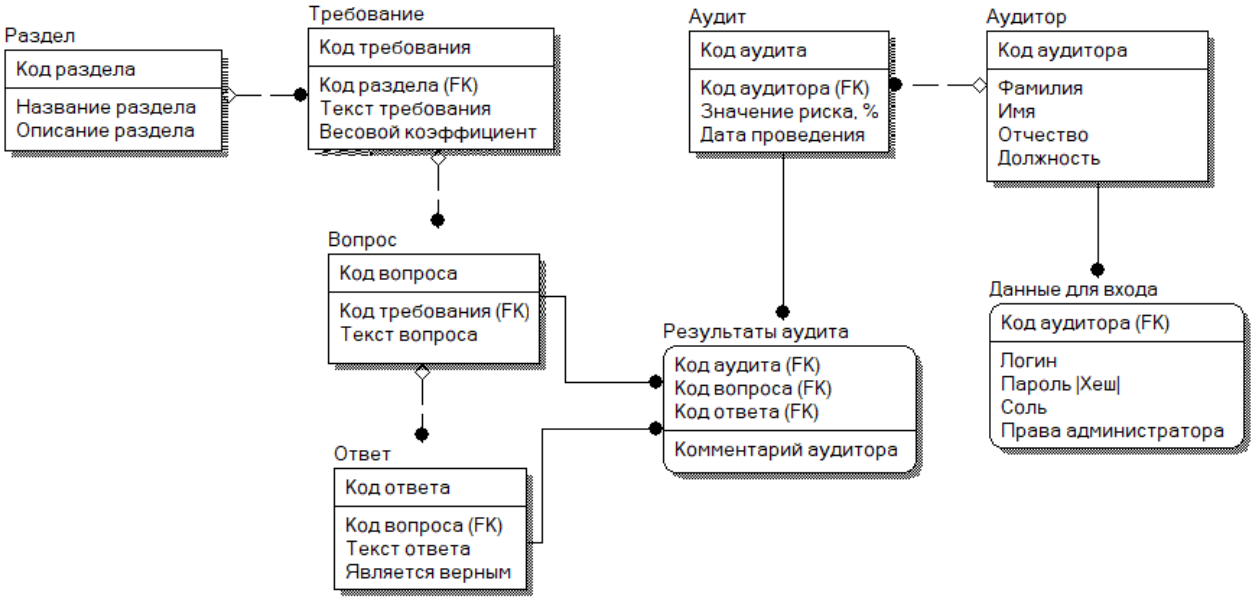

Рисунок 32 – Логическая модель БД (IDEF1X)

2.5.3 Физическое проектирование

Физическая модель базы данных строится на основе логической модели. Проектирование структуры данных предполагает построение для каждого отношения таблицы. Ниже представлены такие таблицы.

Таблица 9 - Физическая структура данных отношения «Раздел»

Название атрибута	Тип атрибута	Условия	Формат данных	Индексация
Код раздела	Числовой	>0	Integer	Primary key
Название раздела	Текстовый	-	Nvarchar(100)	-
Описание раздела	Текстовый	-	Nvarchar(300)	-

Таблица 10 - Физическая структура данных отношения «Требование»

Название атрибута	Тип атрибута	Условия	Формат данных	Индексация
Код требования	Числовой	>0	Integer	Primary key
Код раздела	Числовой	>0	Integer	Foreign key
Текст требования	Текстовый	-	Nvarchar(500)	-
Весовой коэффициент	Логический		Boolean	-

Таблица 11 - Физическая структура данных отношения «Вопрос»

Название атрибута	Тип атрибута	Условия	Формат данных	Индексация
Код вопроса	Числовой	>0	Integer	Primary key
Код требования	Числовой	>0	Integer	Foreign key
Текст вопроса	Текстовый	-	Nvarchar(300)	-

Таблица 12 - Физическая структура данных отношения «Ответ»

Название атрибута	Тип атрибута	Условия	Формат данных	Индексация
Код ответа	Числовой	>0	Integer	Primary key
Код вопроса	Числовой	>0	Integer	Foreign key
Текст ответа	Текстовый	-	Nvarchar(500)	-
Является верным	Логический	-	Boolean	-

Таблица 13 - Физическая структура данных отношения «Аудит»

Название атрибута	Тип атрибута	Условия	Формат данных	Индексация
Код аудита	Числовой	>0	Integer	Primary key
Код аудитора	Числовой	>0	Integer	Foreign key
Дата проведения	Дата/Время	-	dd.mm.yyyy hh:mm:ss	-
Значение риска, %	Числовой	>=0	Float	-

Таблица 14 - Физическая структура данных отношения «Результаты аудита»

Название атрибута	Тип атрибута	Условия	Формат данных	Индексация
Код аудита	Числовой	>0	Integer	Primary key
Код ответа	Числовой	>0	Integer	Primary key
Код вопроса	Числовой	>0	Integer	Primary key
Комментарий аудитора	Текстовый	-	Nvarchar(500)	

Таблица 15 - Физическая структура данных отношения «Аудитор»

Название атрибута	Тип атрибута	Условия	Формат данных	Индексация
Код аудитора	Числовой	>0	Integer	Primary key
Фамилия	Текстовый	-	Nvarchar(50)	-
Имя	Текстовый	-	Nvarchar(50)	-
Отчество	Текстовый	-	Nvarchar(50)	-
Должность	Текстовый	-	Nvarchar(50)	-

Таблица 16 - Физическая структура данных отношения «Данные для входа»

Название атрибута	Тип атрибута	Условия	Формат данных	Индексация
Код аудитора	Числовой	>0	Integer	Primary key
Логин	Текстовый	-	Varchar(15)	-
Пароль (Хеш)	Текстовый	-	Varchar(128)	-
Соль	Текстовый	-	Varchar(100)	-
Права администратора	Логический	-	Boolean	-

Результатом физического проектирования БД является физическая модель БД в нотации IDEF1X, представленная на рисунке 33.

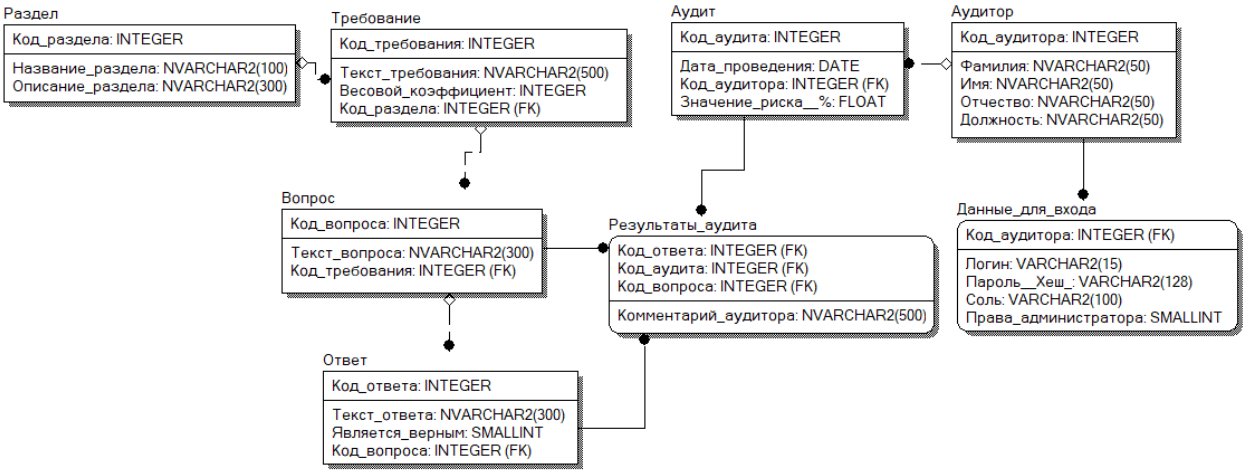

Рисунок 33 – Физическая модель БД (IDEF1X)

3 ОПИСАНИЕ РАЗРАБОТАННОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

3.1 Список основных сведений

Общие сведения

Программа разработана в среде Microsoft Visual Studio Community 2019. БД разработана с использованием phpMyAdmin.

Функциональное назначение

Разрабатываемое программное обеспечение направлено на решение следующих задач:

- автоматизация процесса проведения аудита информационной безопасности;

- осуществление анализа рисков ИБ;

- проверка соответствия существующей политики безопасности на соответствие стандарту ГОСТ Р ИСО/МЭК 27002-2012;

Используемые технические средства

Программа предназначена для работы на IBM-совместимых персональных компьютерах, имеющих следующие минимальные характеристики: тактовая частота процессора не ниже 1,8 ГГц; 2 ГБ ОЗУ;
800 Мб на жёстком диске;

Входные данные

Источником входных данных для программы является база данных, содержащая таблицы: «Раздел», «Требование», «Вопрос», «Ответ», «Аудит», «Результаты аудита», «Аудитор», «Данные для входа».

Выходные данные

Выходными данными являются результаты проведённых аудитов, включая значения рисков.

3.2 Логическая структура

Программа состоит из 8 основных модулей:

- главный модуль;
- модуль проведения тестирования;
- модуль представления результатов;
- модуль редактирования данных;
- модуль расчёта риска;
- модуль анализа рисков;
- модуль управления списком пользователей;
- модуль формирования отчётов.

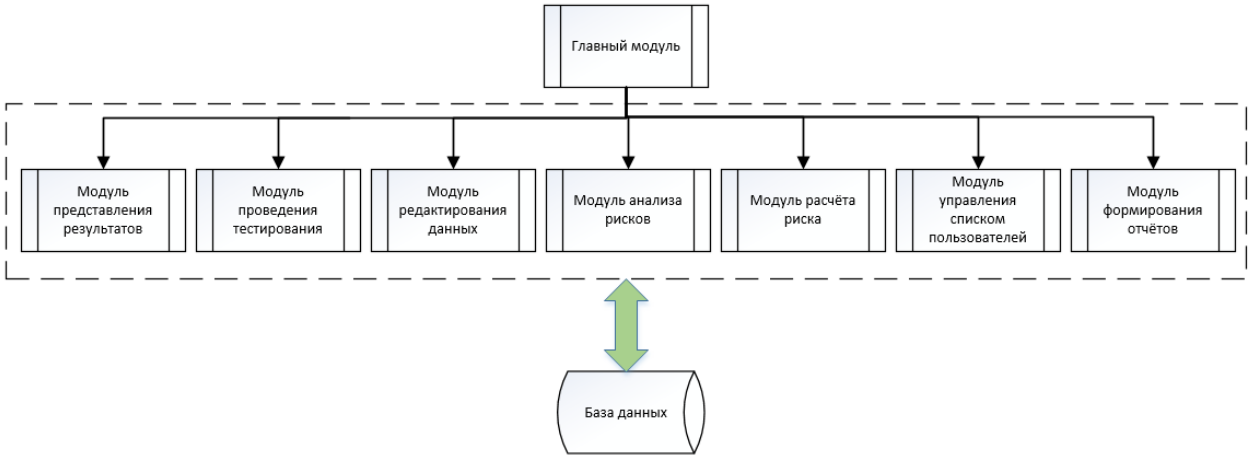

Рисунок 34 – Структура программы

3.2.1 Главный модуль

Главный модуль программы предоставляет пользователю интерфейс для выбора предусмотренных программой действий и, соответственно, перехода к другим программным модулям.

Основные функции данного модуля:

- отображение интерфейса для перехода к другим программным модулям;
- отображение статистических данных по результатам ранее проведённых аудитов;

- отображение основных данных ранее проведённых аудитов (дата проведения, ФИО аудитора, количество выполненных и невыполненных требований).

Алгоритм работы главного модуля представлен на рисунке 35.

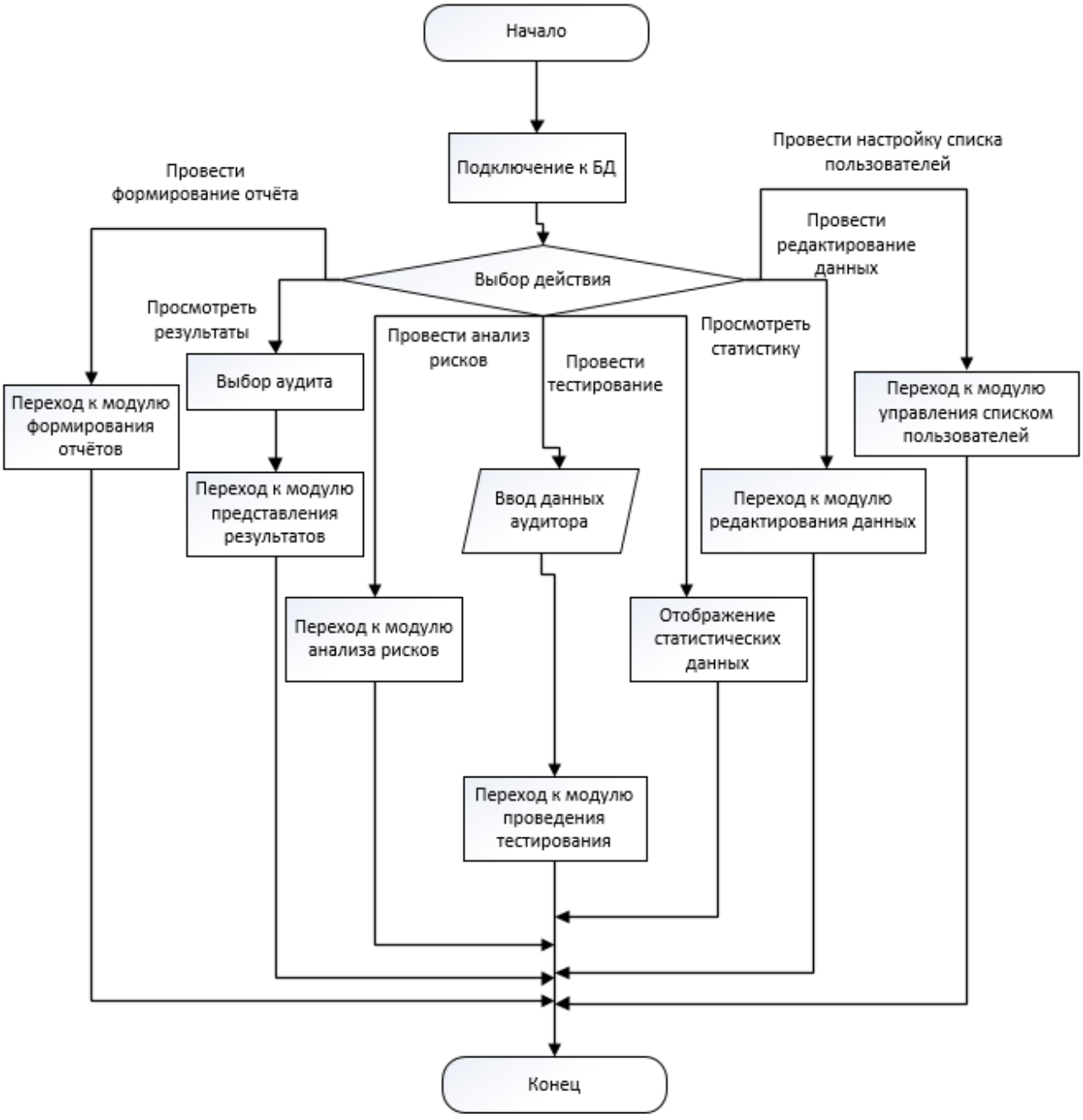

Рисунок 35 - Алгоритм работы главного модуля

3.2.2 Модуль проведения тестирования

Данный модуль предназначен для проведения аудита ИБ в виде теста.

Основные функции этого модуля:

- отображение списка вопросов и соответствующих им ответов;

- предоставление пользователю интерфейса для выбора ответов на каждый вопрос;

- сохранение результатов тестирования и добавление их в базу данных;

Алгоритм работы модуля представлен на рисунке

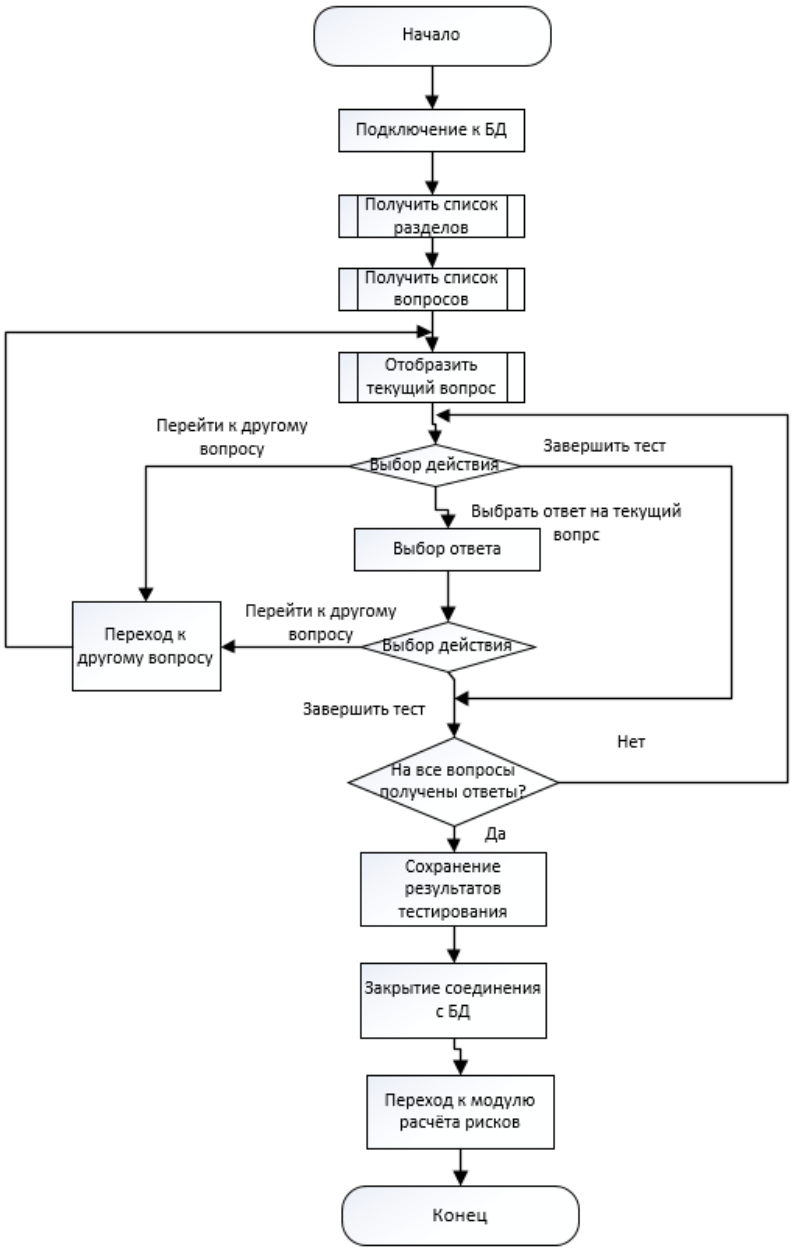

Рисунок 36 – Алгоритм работы модуля проведения тестирования

3.2.3 Модуль представления результатов

Данный модуль предназначен для отображения результатов определённого аудита.

Функции модуля:

- отображение основных данных аудита (дата проведения, ФИО аудитора);

- отображение списка выполненных и невыполненных требований;

- отображение подробных результатов по выбранному требованию (связанный вопрос и список выбранных ответов, комментарий аудитора).

Алгоритм работы модуля представлен на рисунке

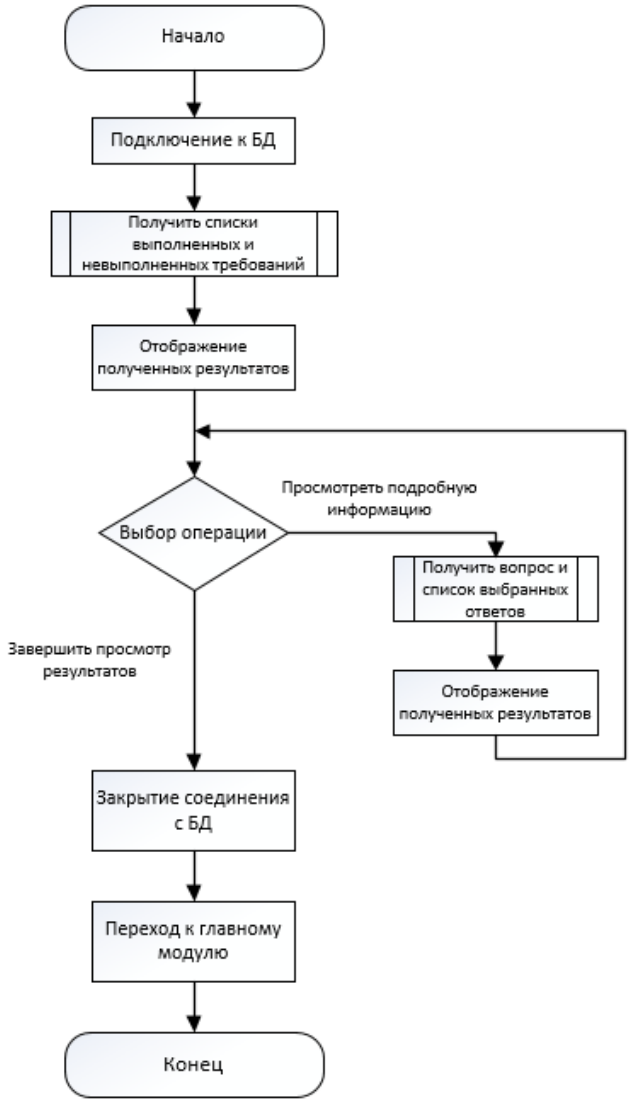

Рисунок 37 – Алгоритм работы модуля представления результатов

3.2.4 Модуль редактирования данных

Данный модуль предназначен для редактирования списка требований, а также разделов тестирования, вопросов и соответствующих им ответов.

Функции модуля:

- добавление, изменение и удаление требований;

- добавление, изменение и удаление разделов;

- добавление, изменение, удаление вопросов и соответствующих им ответов;

- сохранение проведённых изменений в базе данных.

Алгоритм работы модуля представлен на рисунке

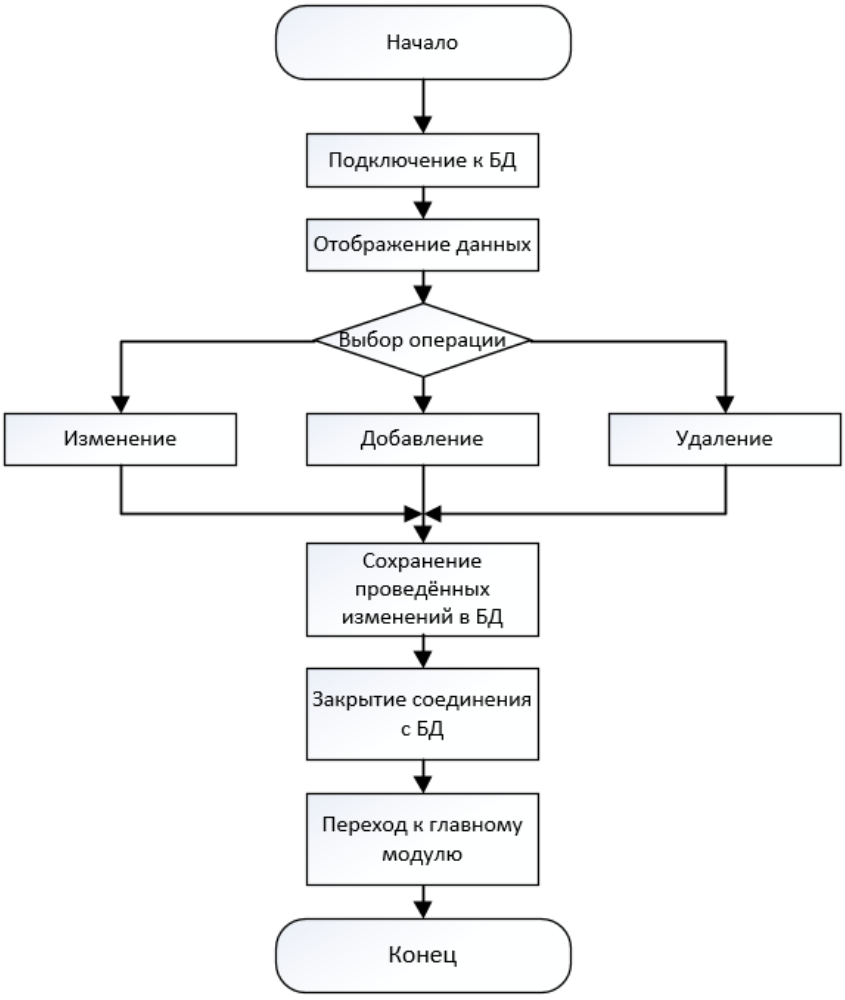

Рисунок 38 – Алгоритм работы модуля редактирования данных

3.2.5 Модуль расчёта риска

Главная функция, выполняемая данным модулем, - вычисление значения риска, связанного с невыполнением требований ИБ.

Вычисляемое значение риска зависит от установленного каждому требованию весового коэффициента V(1-100), характеризующему степень критичности

данного требования для поддержания необходимого уровня защищенности.

В данном модуле происходит расчёт значения риска по следующей формуле:

$$R = \frac{\sum_{i=1}^{n} V_{\text{невып.},i}}{V_{max}}, \quad (1)$$

где $V_{\text{невып., i}}$ – сумма весов невыполненных требований;

V_{max} – сумма весов всех требований.

Т.е. риск равен отношению суммы весов невыполненных требований к сумме весов всех требований.

Алгоритм работы модуля представлен на рисунке

Рисунок 39– Алгоритм работы модуля расчёта рисков

3.2.6 Модуль анализа рисков

Данный модуль предназначен для представления списка рисков по каждому проведённому аудиту с указанием их значения и степени.

Функции модуля:

- представление списка значений рисков для каждого проведённого аудита;
- рассмотрение значений рисков по каждому разделу аудита.

Алгоритм работы модуля представлен на рисунке

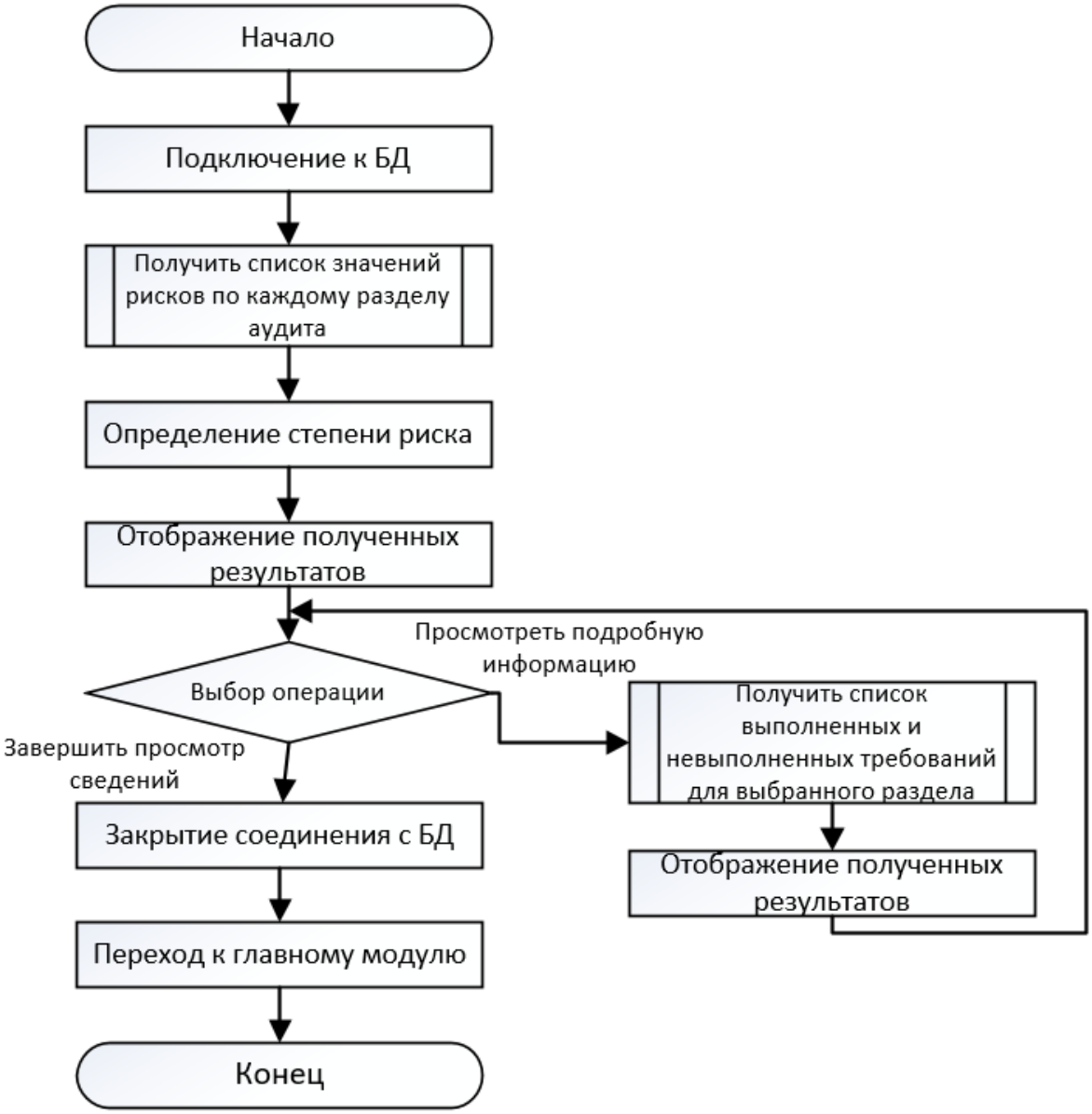

Рисунок 40 - Алгоритм работы модуля анализа рисков

3.2.7 Модуль формирования отчётов

Этот модуль предназначен для формирования отчётов по результатам проведённых ранее аудитов в формате .xls.

Функции данного модуля:

- настройка содержимого отчёта;
- формирование отчёта.

Алгоритм работы модуля представлен на рисунке

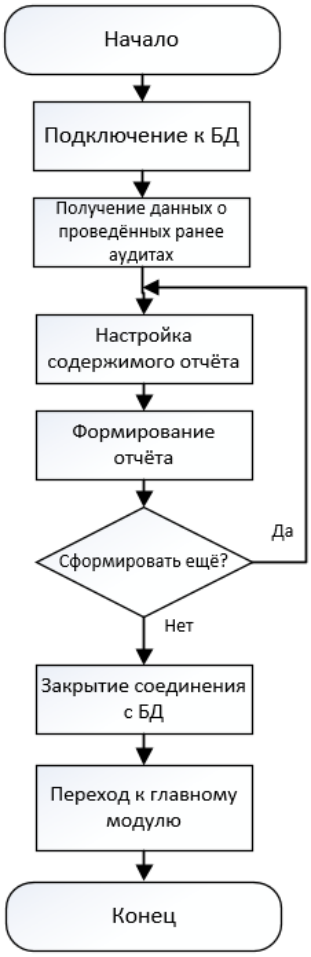

Рисунок 41 – Алгоритм работы модуля формирования отчётов

3.2.8 Модуль управления списком пользователей

Данный модуль предназначен для редактирования списка пользователей, включая добавление новых пользователей, редактирование и удаление данных уже добавленных пользователей.

Функции модуля:

- отображение списка пользователей с указанием логина и ФИО;

- изменение логинов, паролей, а также прав доступа уже добавленных пользователей;

- добавление новых пользователей;

- удаление добавленных ранее пользователей;

Алгоритм работы модуля по большей части аналогичен алгоритму работы модуля редактирования данных, представленному на рисунке 38.

3.3 Установка и настройка локального сервера

Для того чтобы начать использовать программу сначала необходимо провести установку локального сервера MAMP. Загрузить файл установки можно с официального сайта. После этого нужно запустить файл и провести установку программы в любую папку.

После открытия MAMP через исполняемый файл в директории необходимо запустить Apache Server и MySQL Server, отметив соответствующие флажки в правом верхнем углу.

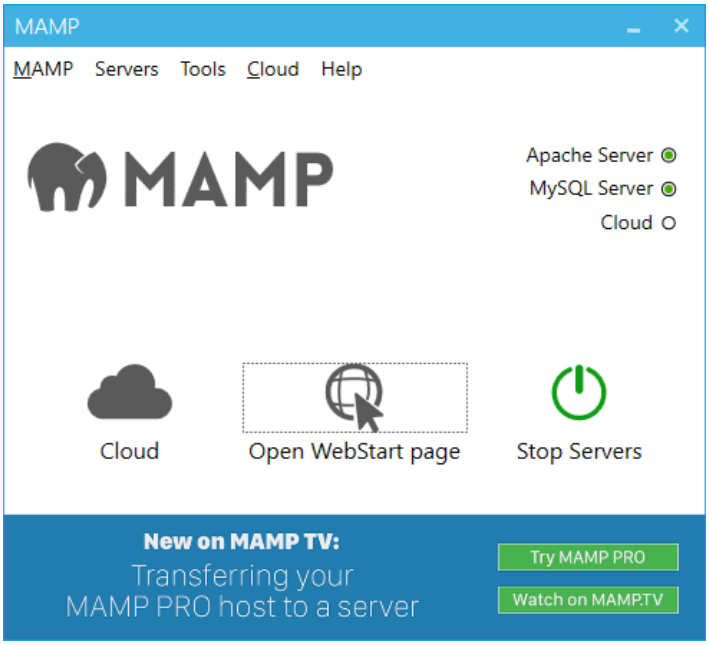

Рисунок 42 – Главное окно MAMP

Затем нужно открыть главную страницу, выбрав пункт «Open WebStart page». После открытия страницы необходимо перейти в инструменты (Tools) и выбрать phpMyAdmin. В результате будет открыта страница, предоставляющая доступ интерфейсу веб-приложения phpMyAdmin, используемого для администрирования БД.

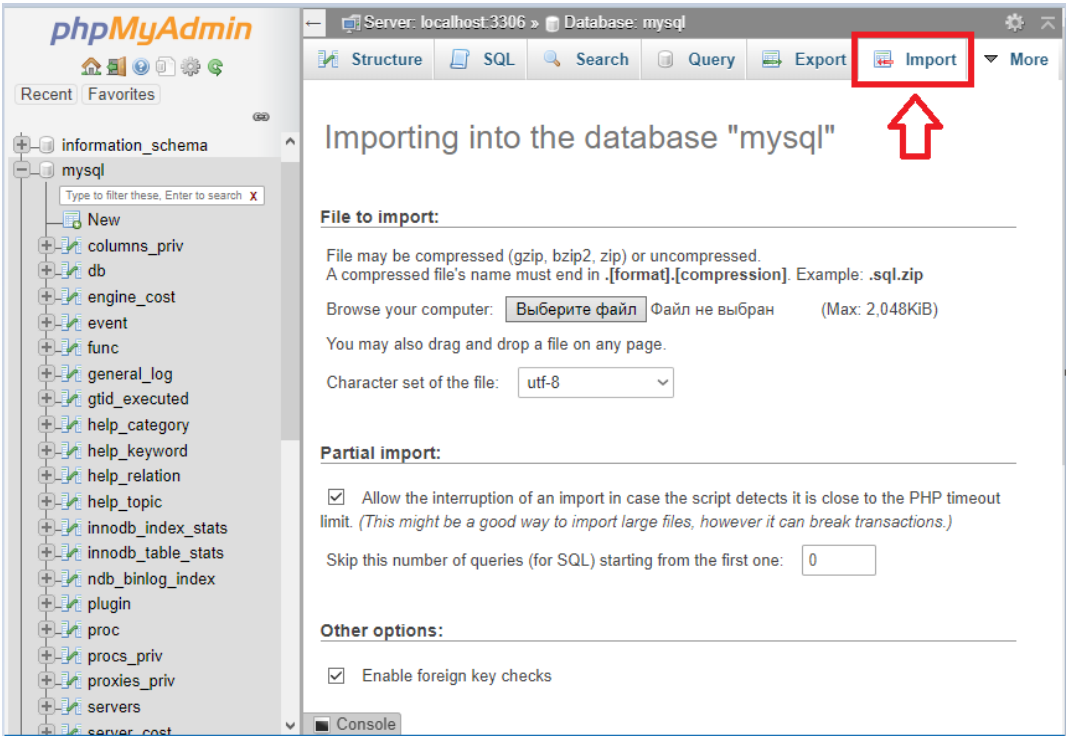

Рисунок 43 – Импорт базы данных

Далее необходимо импортировать базу данных testdata.sql. Для этого сначала нужно создать базу данных с таким же названием (testdata), выбрав пункт «New» в левой области приложения, где расположен список всех баз данных. После создания новой БД необходимо выделить её название и выбрать пункт «Import», а затем в открывшемся окне выбрать файл testdata.sql, нажав на кнопку «Выберите файл».

4 РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ

4.1 Авторизация

Для начала работы с программой пользователю необходимо пройти авторизацию, введя свой логин и пароль и нажав на кнопку «Войти». Форма авторизации представлена на рисунке 44.

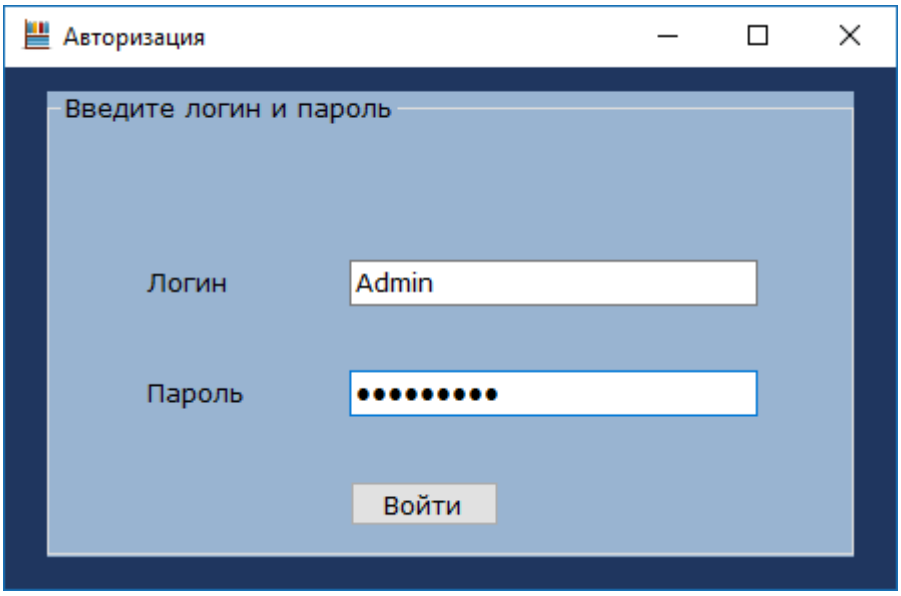

Рисунок 44 – Окно авторизации

В случае ввода пользователем неправильного логина или пароля, ему будет выдано соответствующее сообщение об ошибке.

4.1 Проведение аудита

После прохождения авторизации на экране появляется главное окно, представленное на рисунке 45. На главной форме расположено меню, имеющее пункты: «Просмотр результатов», «Просмотр статистики», «Анализ рисков», «Сформировать отчёт», «Настройка требований», «Настройка пользователей» (только для администратора).

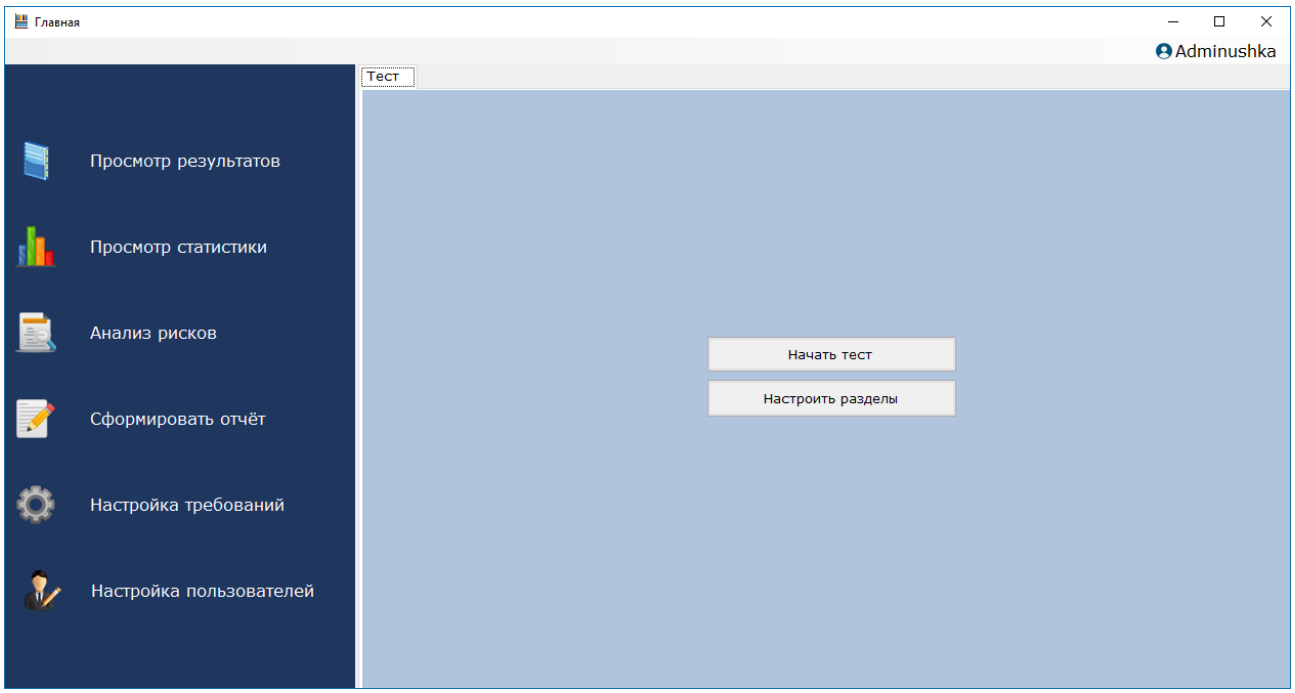

Рисунок 45 – Главное окно программы

Пользователь имеет возможность настроить разделы тестирования, выбрав только те, которые ему необходимы. Для открытия окна настройки необходимо нажать на кнопку «Настроить разделы». В результате будет открыта форма, представленная на рисунке 46. После выполнения настройки необходимо нажать на кнопку «Сохранить изменения».

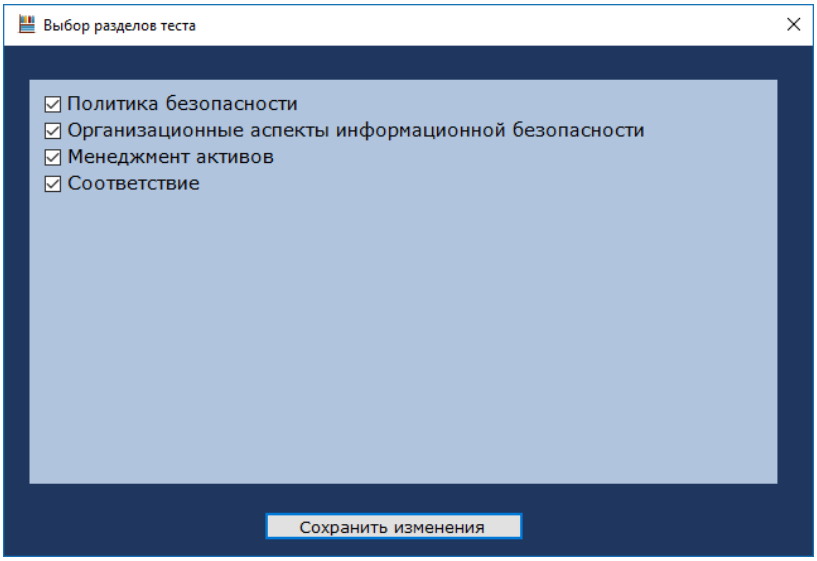

Рисунок 46 - Настройка разделов тестирования

Для начала тестирования необходимо нажать на кнопку «Начать тест». В результате будет открыто новое окно с тестом, представленное на рисунке 47.

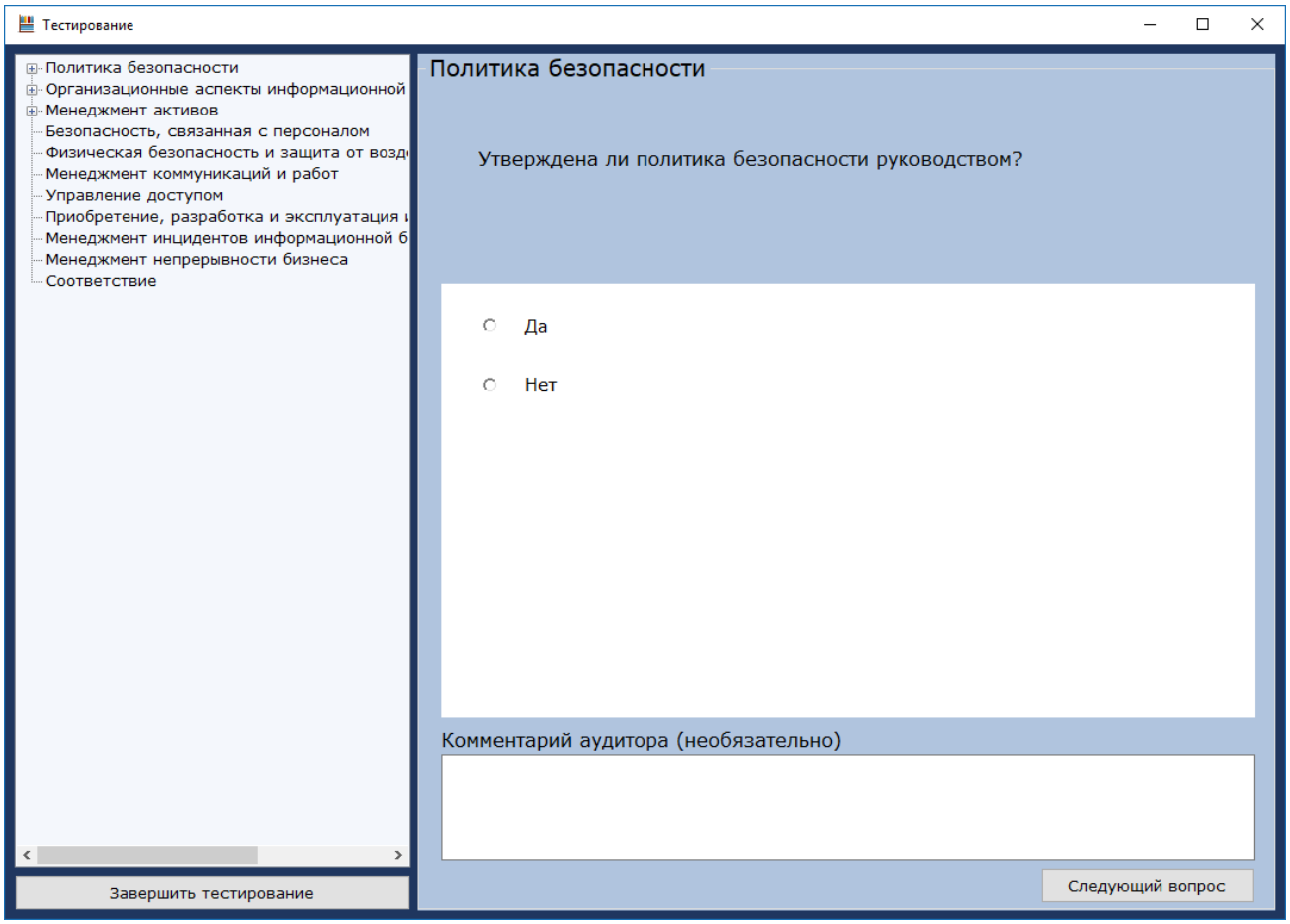

Рисунок 47 - Проведение тестирования

Переключаться между вопросами можно путём нажатия на кнопки «Следующий вопрос» и «Предыдущий вопрос», а также путем непосредственного выбора нужного вопроса из списка, расположенного в левой части формы.

Существует два типа вопросов: с возможностью выбора только одного ответа и с несколькими ответами. Для выбора ответа необходимо установить флажок напротив нужного варианта.

Также при проведении тестирования имеется возможность добавить комментарий к любому отвеченному вопросу. Для этого необходимо в поле «Комментарий аудитора» вписать нужный текст.

Для завершения тестирования необходимо нажать на кнопку «Завершить тестирование». В случае, если на некоторые вопросы ответы были не даны, будет выдано соответствующее сообщение. В противном случае тестирование будет завершено и аудитору будет предоставлено окно с результатами. Просмотр результатов тестирования будет подробнее рассмотрен в следующей главе.

4.2 Проведение анализа рисков

Для проведения анализа рисков необходимо выбрать пункт меню «Анализ рисков». После этого пользователю будет предоставлен список всех ранее проведённых аудитов с указанием значения риска (в процентах), а также степень риска (низкий, средний, высокий).

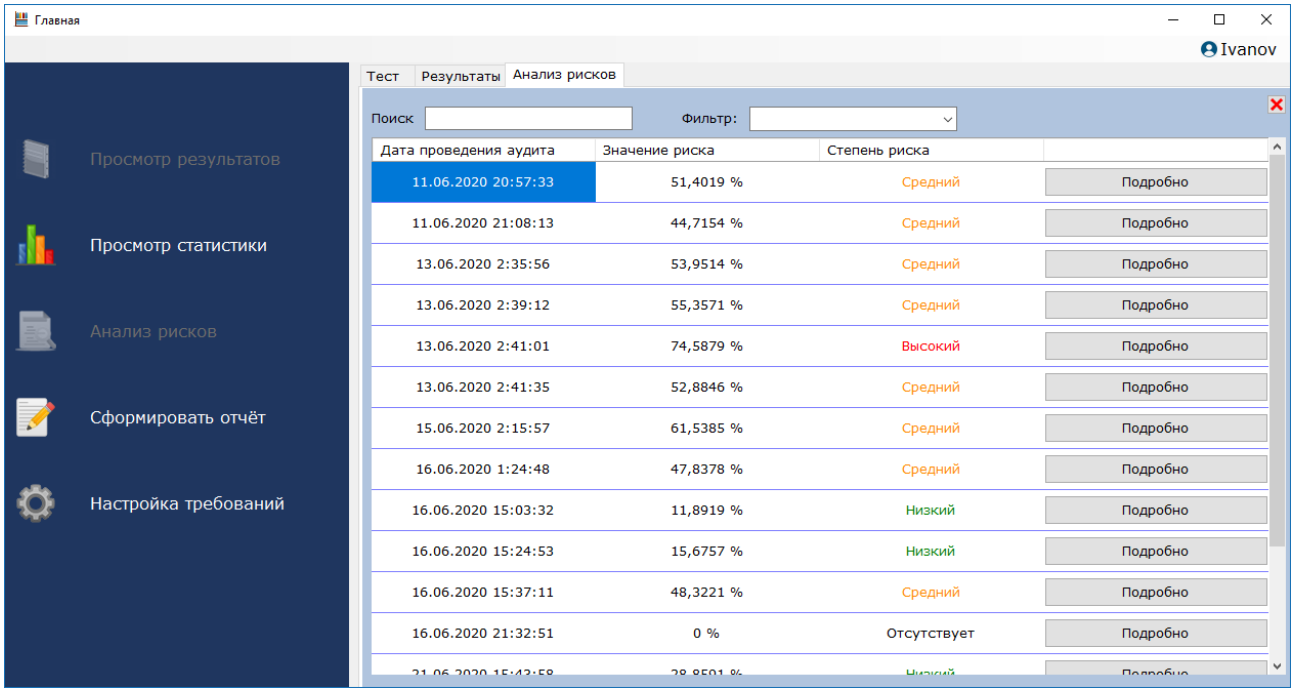

Рисунок 48 -Список рисков

Для просмотра более подробной информации по определённому аудиту необходимо нажать на кнопку «Подробно». После этого откроется форма, где будет представлен список всех разделов, включённых в данную проверку, с указанием значения и степени риска для каждого из разделов.

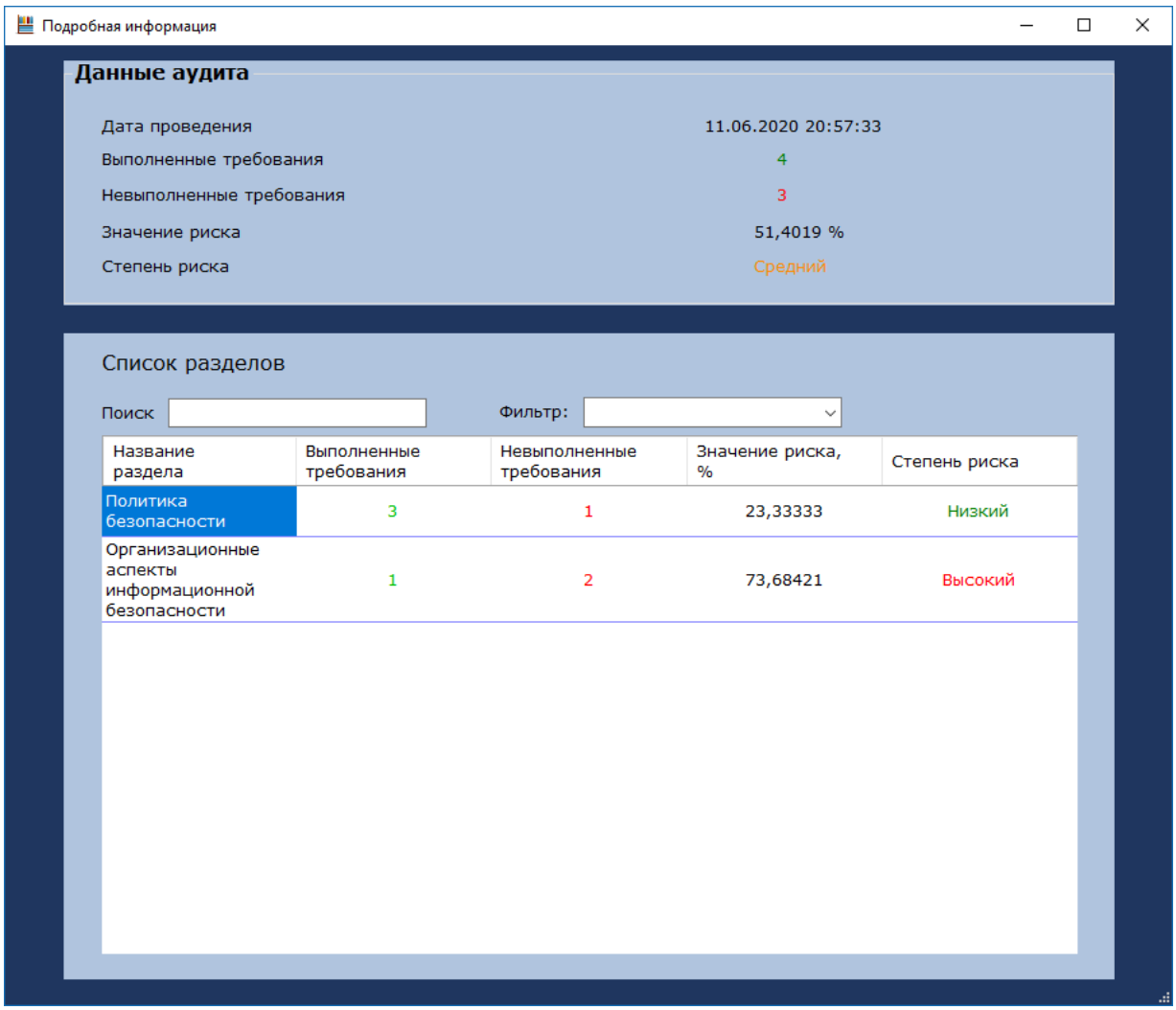

Рисунок 49 - Просмотр рисков по разделам

Для того, чтобы просмотреть список выполненных и невыполненных требований в определённом разделе, необходимо два раза щёлкнуть мышью по названию нужного раздела. После этого будет открыта соответствующая форма

4.3 Просмотр результатов тестирования

Для просмотра результатов всех проводимых тестов необходимо выбрать пункт меню «Просмотр результатов» на главном окне программы. После выбора данного пункта будет открыта вкладка программы, содержащая краткую информацию о всех проведенных проверках, включая дату проведения, ФИО аудитора, а также количество выполненных и невыполненных требований.

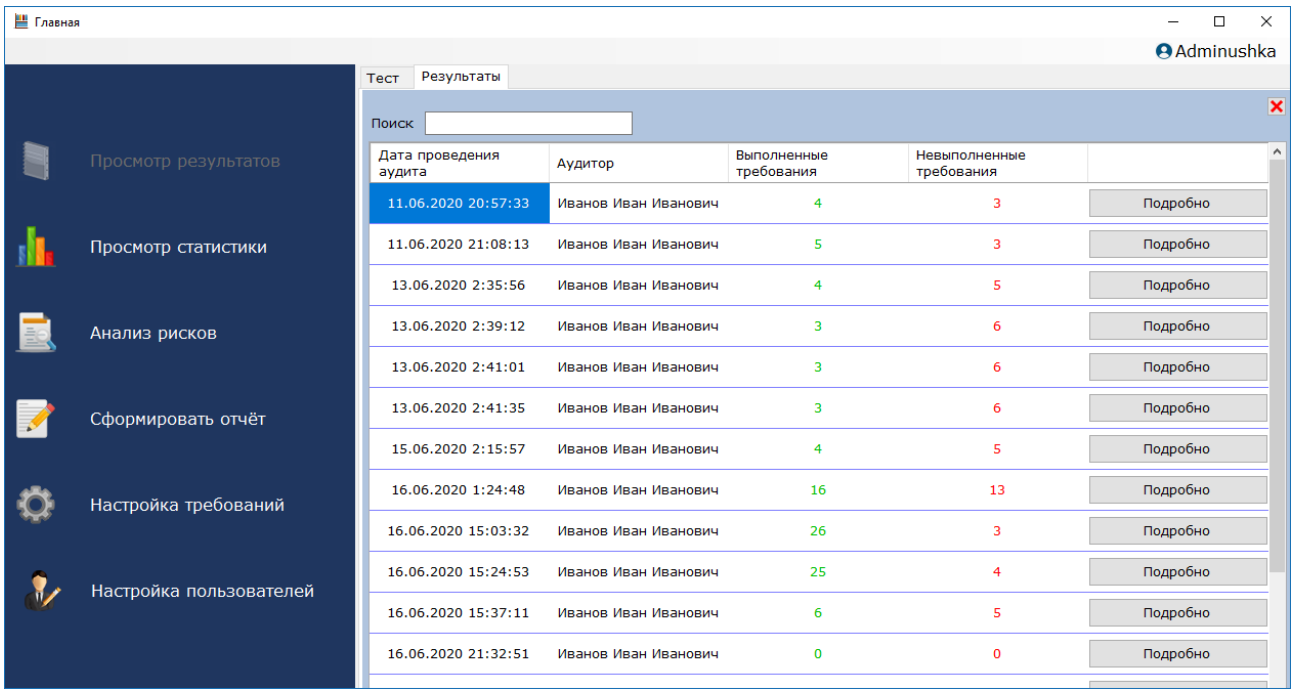

Рисунок 50 - Просмотр результатов тестирования

Для просмотра подробной информации необходимо нажать на кнопку «Подробно» напротив нужного результата. После этого появится то же самое окно, что и в случае завершения тестирования, содержащее список выполненных и невыполненных требований.

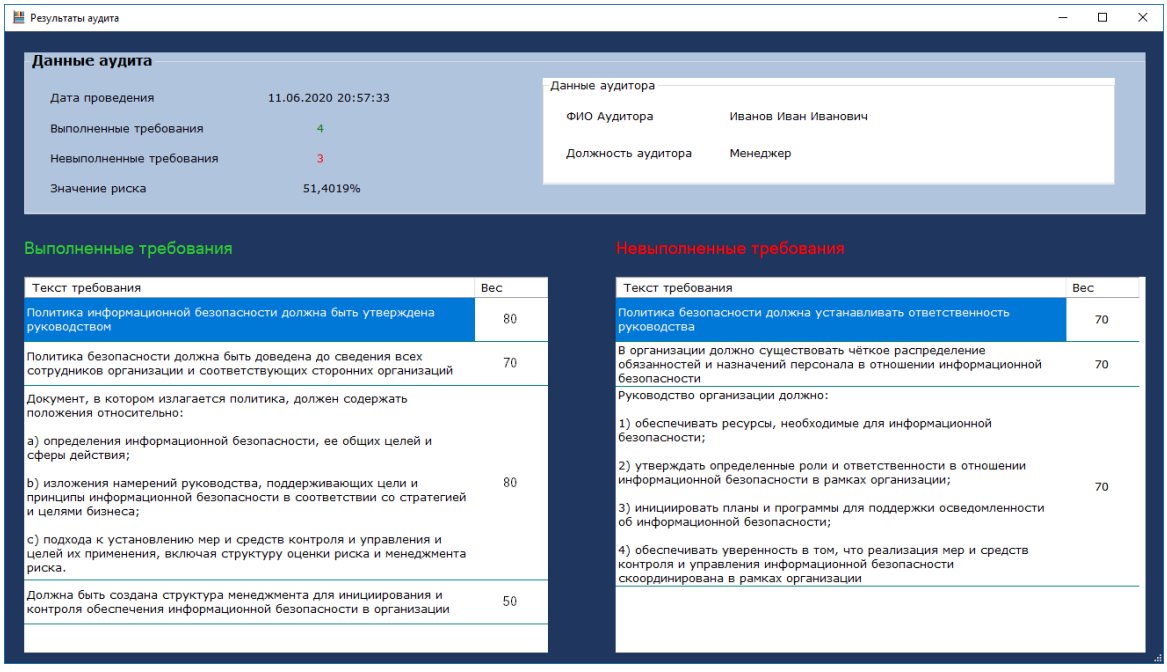

Рисунок 51 - Просмотр выполненных и невыполненных требований

Для того чтобы увидеть информацию о выбранных в ходе тестирования ответах, необходимо произвести двойной щелчок мыши на нужном требовании. После этого будет открыто окно, содержащее текст вопроса, связанного с этим требованием, список ответов, с указанием их правильности, а также текст комментария аудитора, если такой имеется. Ответы, которые были не выбраны аудитором, но которые необходимо было выбрать, отмечаются восклицательным знаком.

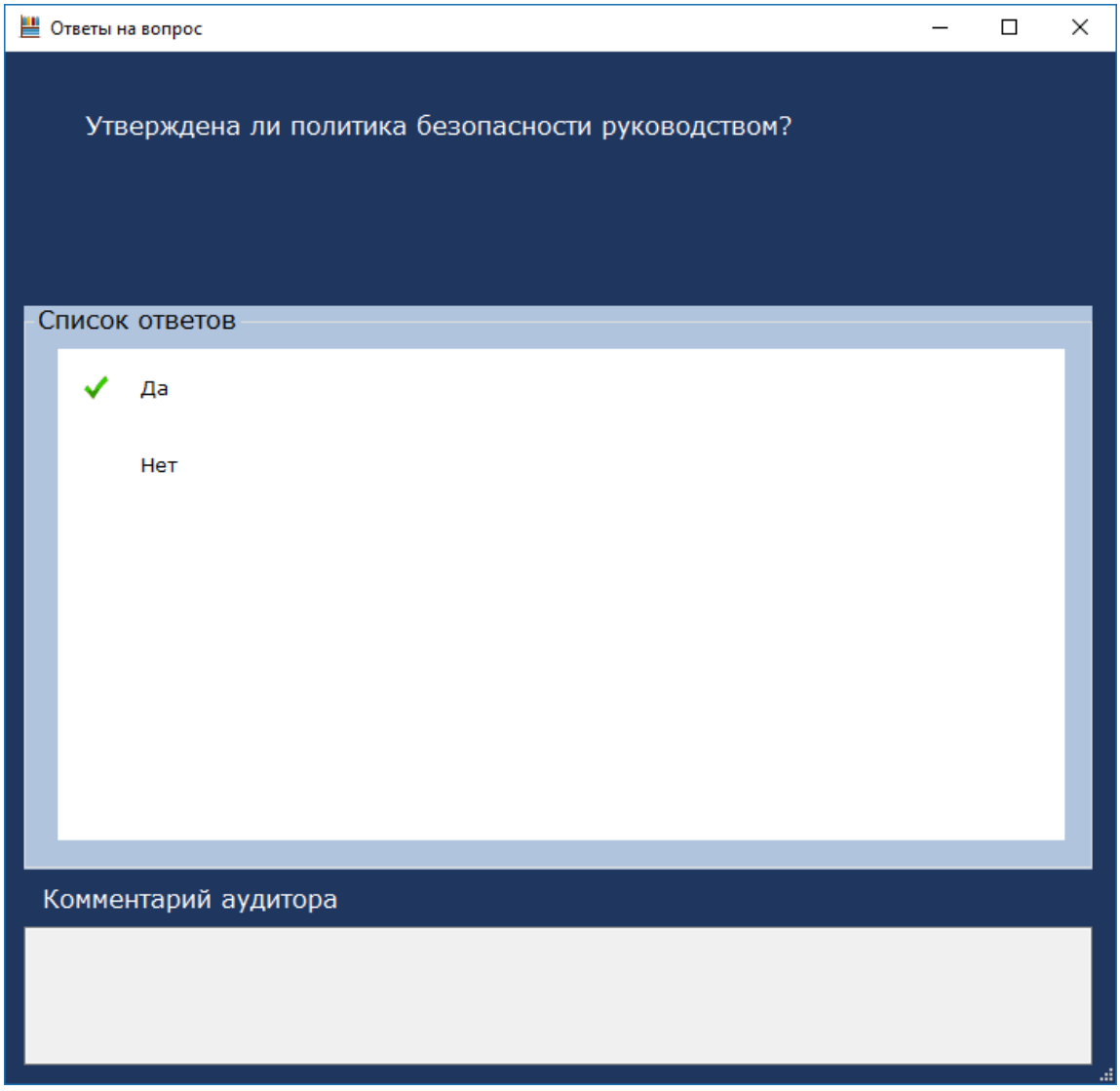

Рисунок 52 – Просмотр ответов на вопрос

4.4 Просмотр статистики

Для просмотра статистических данных необходимо выбрать пункт меню «Просмотр статистики». После этого будет открыта вкладка, содержащая результаты тестов, представленные в виде диаграммы. Изначально отображаются результаты последних шести проведённых проверок. Для просмотра более ранних результатов необходимо нажать на кнопку «Предыдущие результаты».

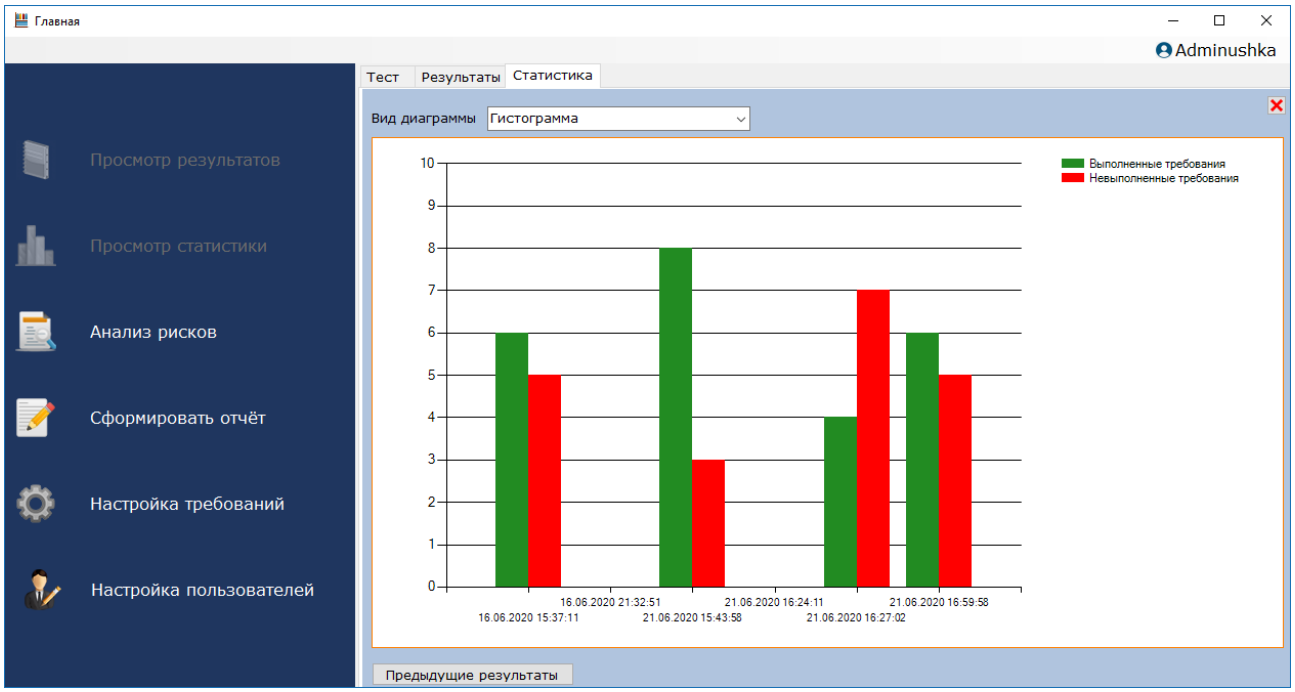

Рисунок 53 - Просмотр статистики

Изменить вид диаграммы можно путём выбора соответствующего пункта выпадающего списка «Вид диаграммы». Можно выбрать один из четырех разных типов: гистограмма, линейчатая диаграмма, гистограмма с накоплением, линейчатая диаграмма с накоплением.

4.5 Формирование отчётов

Для того чтобы перейти к окну формирования отчётов, необходимо выбрать пункт меню «Сформировать отчёт». После этого пользователю будет предоставлена форма, представленная на рисунке 54, где можно настроить содержимое отчёта.

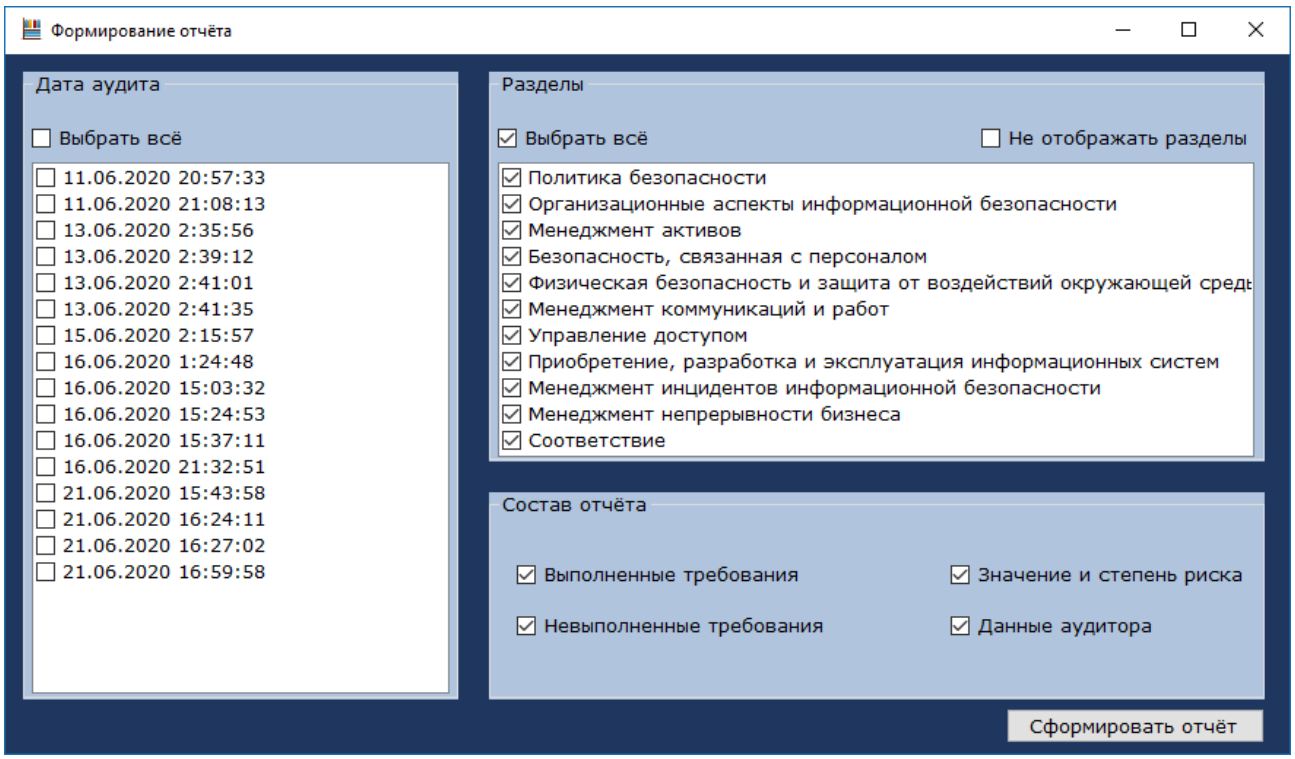

Рисунок 54 – Формирование отчёта

После настройки отчёта необходимо нажать на кнопку «Сформировать отчёт», а затем в открывшемся окне выбрать расположение файла и его имя. В результате выполнения всех перечисленных действий будет сформирован отчёт по результатам аудитов в виде файла Excel. Пример отчёта представлен на рисунке.

Дата проведения	ФИО аудитора	Должность аудитора	Значение риска	Уровень риска
11.06.2020 20:57:33	Иванов Иван Иванович	Менеджер	51,40190125	Средний

Название раздела	Значение риска	Степень риска	Выполненные требования	Невыполненные требования
Политика безопасности	23,33333397	Низкий	Политика информационной безопасности должна быть утверждена руководством	Политика безопасности должна устанавливать ответственность руководства
			Политика безопасности должна быть доведена до сведения всех сотрудников организации и соответствующих сторонних организаций	
			Документ, в котором излагается политика, должен содержать положения относительно: a) определения информационной безопасности, ее общих целей и сферы действия; b) изложения намерений руководства, поддерживающих цели и принципы информационной безопасности в соответствии со стратегией и целями бизнеса;	

Рисунок 55 – Сформированный отчёт

4.5 Редактирование требований

Для осуществления редактирования требований необходимо выбрать пункт меню «Настройка требований». В результате будет открыта форма, где необходимо выбрать в выпадающем списке один из разделов тестирования. После выбора появится таблица, содержащая список требований, входящих в данный раздел. Здесь можно изменить текст любого требования или его весовой коэффициент, удалить ненужное требования либо добавить новое, нажав на кнопку «Добавить новое требование». Для того, чтобы загрузить список требований из файла XML необходимо нажать на кнопку «Загрузить требования», а затем выбрать нужный файл. Также возможно произвести поиск требования, используя строку поиска. После выполнения любых изменений необходимо нажать на кнопку «Сохранить изменения».

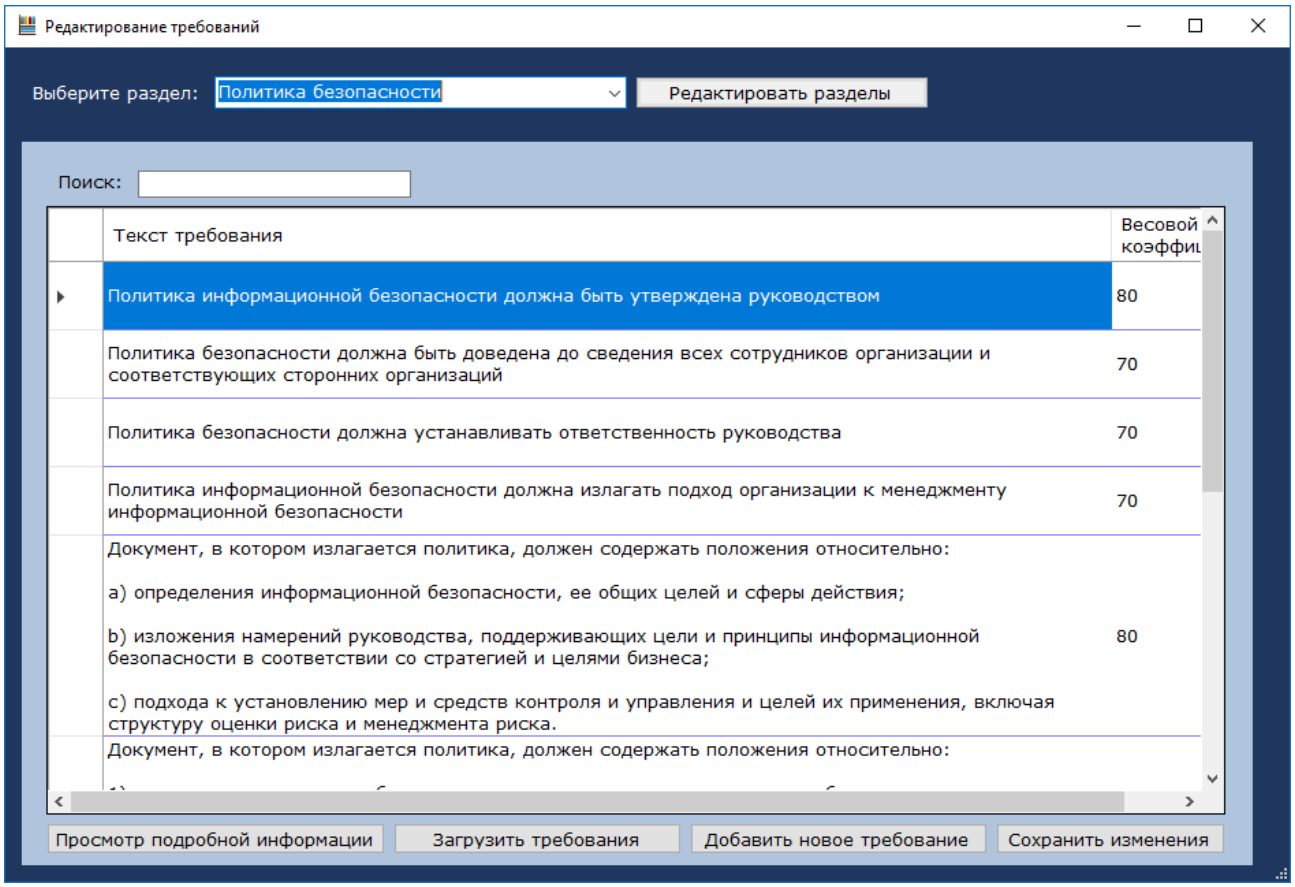

Рисунок 56 - Редактирование требований

Для просмотра более подробной информации о любом требовании необходимо произвести двойной щелчок мышью на нужном требовании либо выделить его и нажать на кнопку «Просмотр подробной информации». После этого будет открыта форма, на которой можно изменить раздел требования, а также произвести редактирование вопроса, связанного с этим требованием, если такой имеется. Также, соответственно, имеется возможность отредактировать существующие ответы на вопрос или добавить новый, нажав на кнопку «Добавить новый ответ». Если же с требованием не связан какой-либо вопрос, то его добавление можно произвести, нажав на кнопку «Добавить новый вопрос».

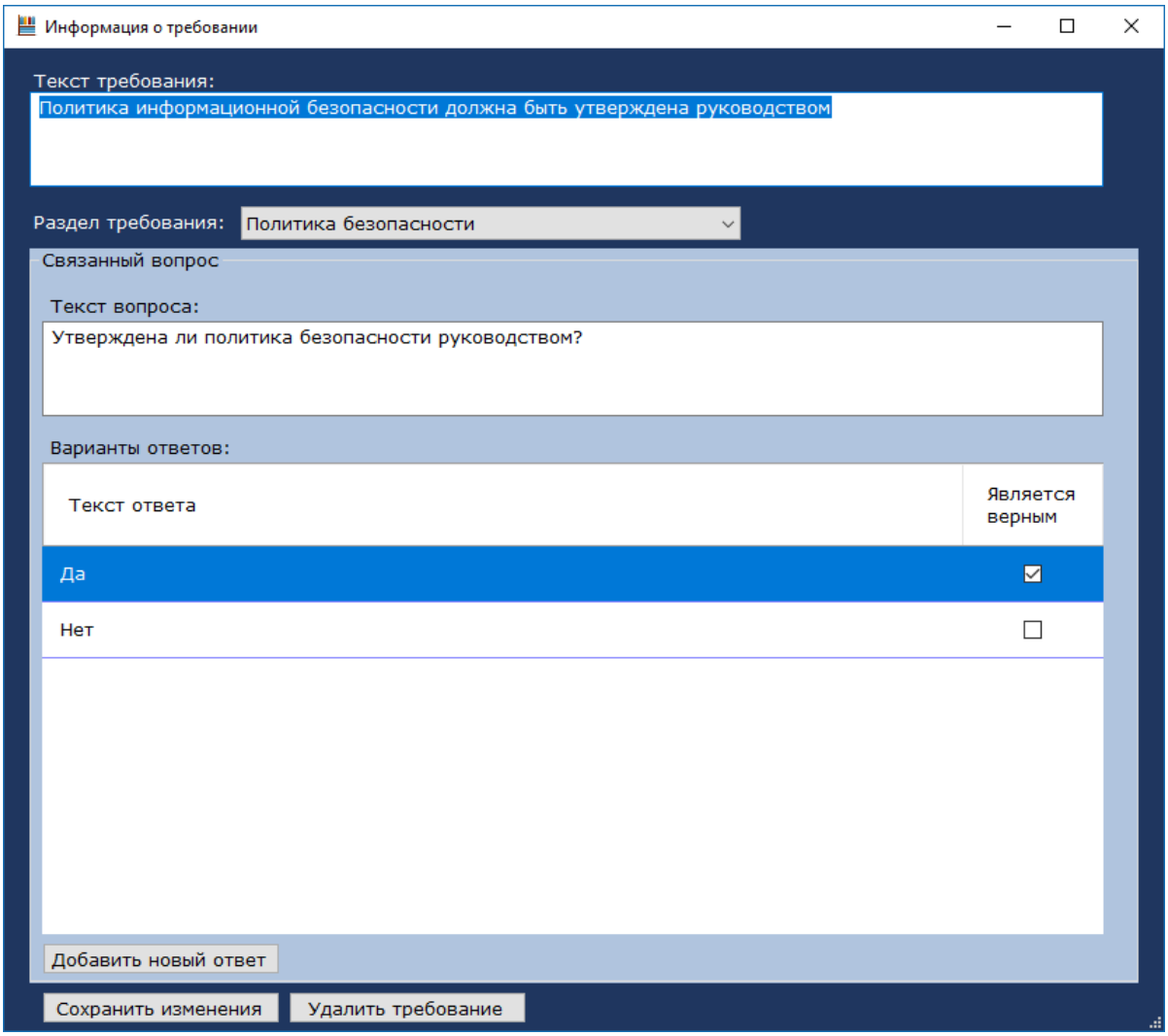

Рисунок 57 - Редактирование списка ответов

Произвести редактирование списка разделов можно, нажав на кнопку «Редактировать разделы» на главном окне редактирования напротив выпадающего списка разделов. После этого будет открыта форма, где можно изменить название уже существующего раздела, произведя по нему двойной щелчок мышью, добавить новый раздел, нажав на кнопку «Добавить», а также удалить ненужный раздел, выделив его мышью и нажав на кнопку «Удалить».

Необходимо отметить, что полное редактирование и удаление возможно только для требований и разделов, добавленных ранее пользователем. Произвести данные операции над предустановленными требованиями и разделами (соответствующими ГОСТ Р ИСО/МЭК 27005-2010) нельзя. Но при этом возможно изменять весовые коэффициенты таких требований.

4.6 Настройка списка пользователей

Пользователям, имеющим права администратора, доступна настройка списка пользователей. В этом случае на панели меню на главной форме программы становится доступен ещё один пункт «Настройка пользователей».

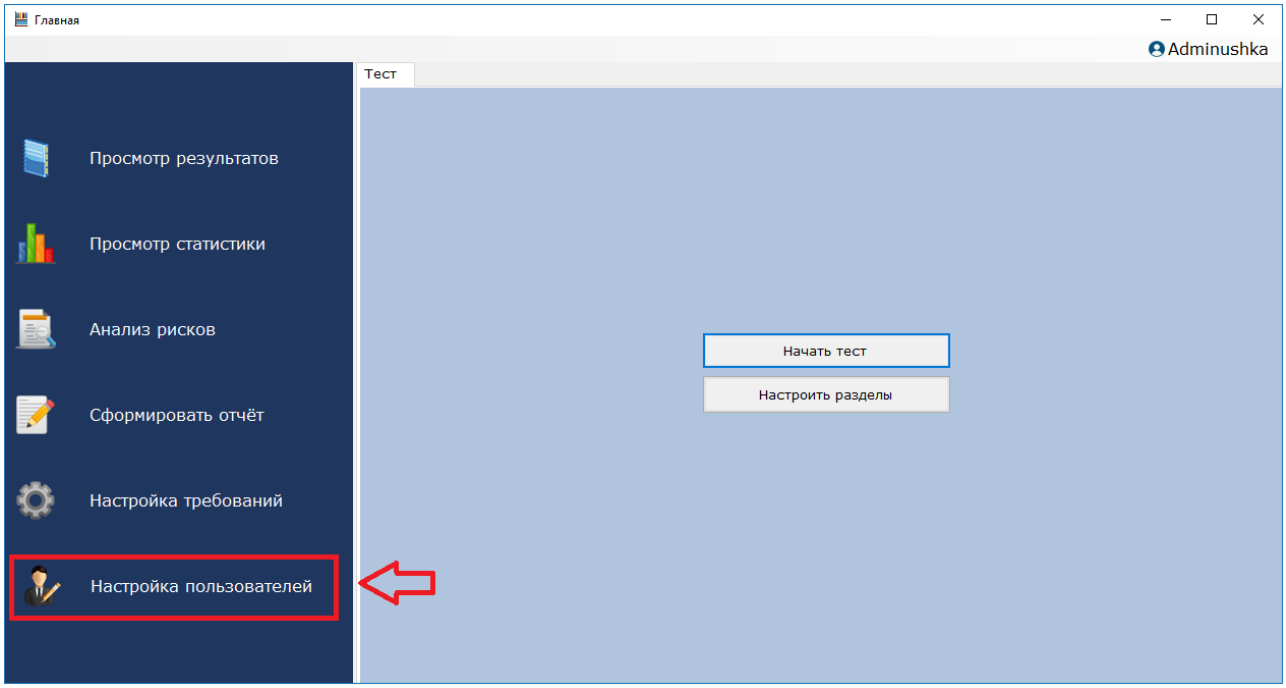

Рисунок 58 – Вид главного окна при входе администратора

После выбора пункта «Настройка пользователей» будет открыта форма, содержащая список пользователей с указанием их ФИО и логина. В данном окне администратор может изменять только логины уже существующих пользователей, а также удалять пользователей. Редактирования данных выполняется путём изменения значения в соответствующей ячейке таблицы. Для удаления данных необходимо выделить строку с нужным пользователем и нажать на клавишу Del либо на кнопку «Удалить». После проведения редактирования данных или удаления необходимо нажать на кнопку «Сохранить» для сохранения изменений.

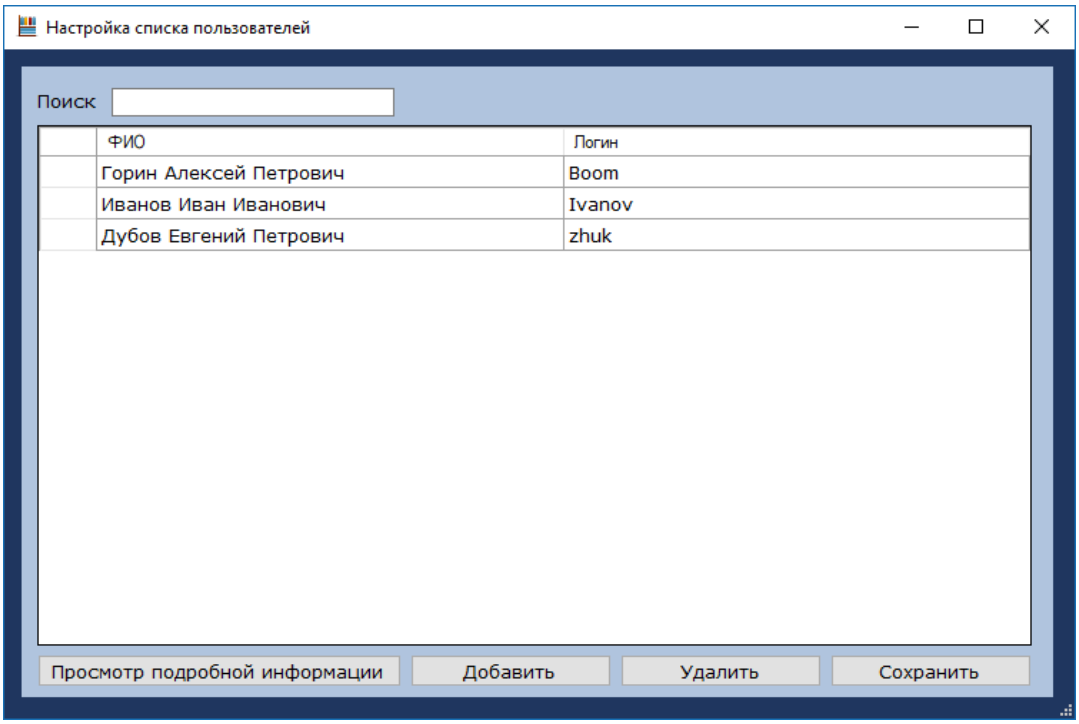

Рисунок 59 - Редактирование списка пользователей

Для того, чтобы изменить пароль пользователя, права доступа или переназначить учётную запись другому аудитору, необходимо щёлкнуть два раза левой кнопкой мыши по строке с нужным пользователем либо выделить строку и нажать на кнопку «Просмотр подробной информации». После этого будет открыта форма, где можно провести соответствующие изменения.

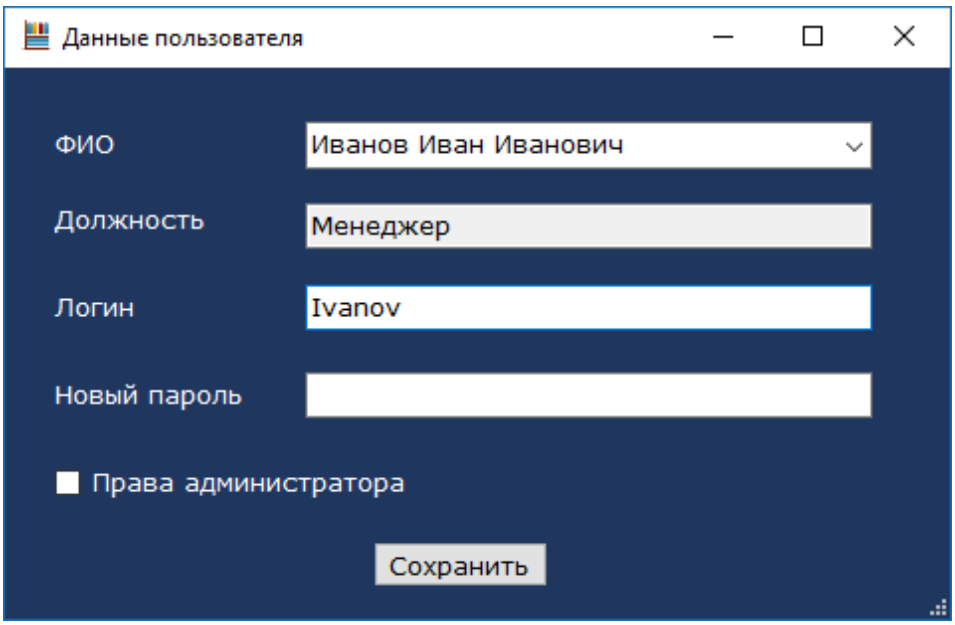

Рисунок 60 - Редактирование данных пользователя

Чтобы добавить нового пользователя, необходимо нажать на кнопку «Добавить» на форме просмотра списка пользователей. После этого будет открыто окно, где можно добавить нового пользователя, заполнив соответствующие поля

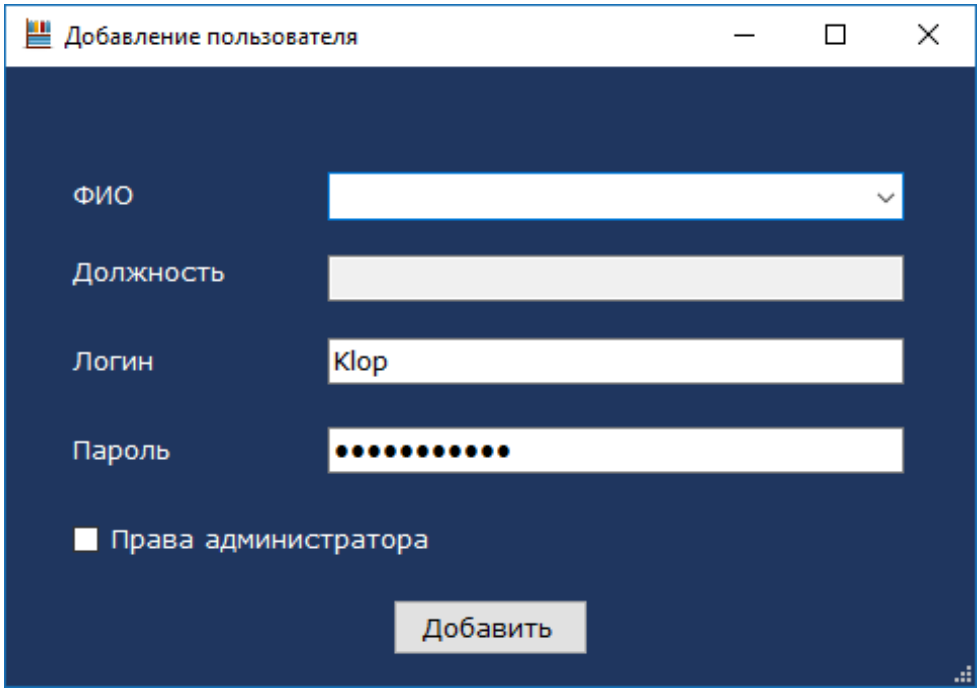

Рисунок 61 – Добавление пользователя

Создаваемая учётная запись может быть назначена только уже имеющемуся в базе данных аудитору. Для добавления нового аудитора необходимо раскрыть выпадающий список «ФИО» и выбрать элемент «Добавить нового работника». После этого будет открыто окно, содержащее соответствующие поля, заполнив которые, можно добавить нового работника в БД.

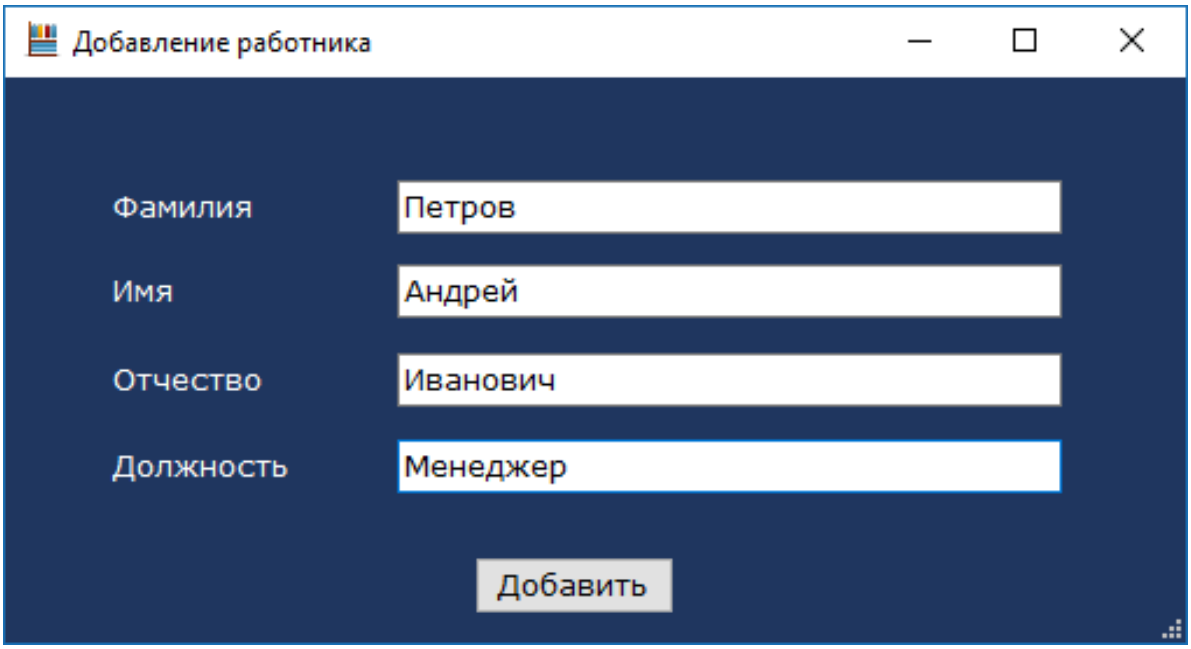

Рисунок 62 – Добавление работника

4.7 Настройка данных пользователя и выход из системы

Для того, чтобы просмотреть данные пользователя, необходимо нажать на имя пользователя в правом верхнем углу экрана и выбрать пункт «Данные пользователя». После этого будет открыто окно, содержащее на первой вкладке личные данные пользователя, а на второй – данные для входа. Пользователь имеет возможность изменить свой логин или пароль, заполнив соответствующие поля на вкладке «Данные для входа» и нажав на кнопку «Сохранить». Если в поля были введены некорректные данные, то пользователю будет выдано соответствующее сообщение. После изменения логина или пароля пользователю будет необходимо авторизоваться заново.

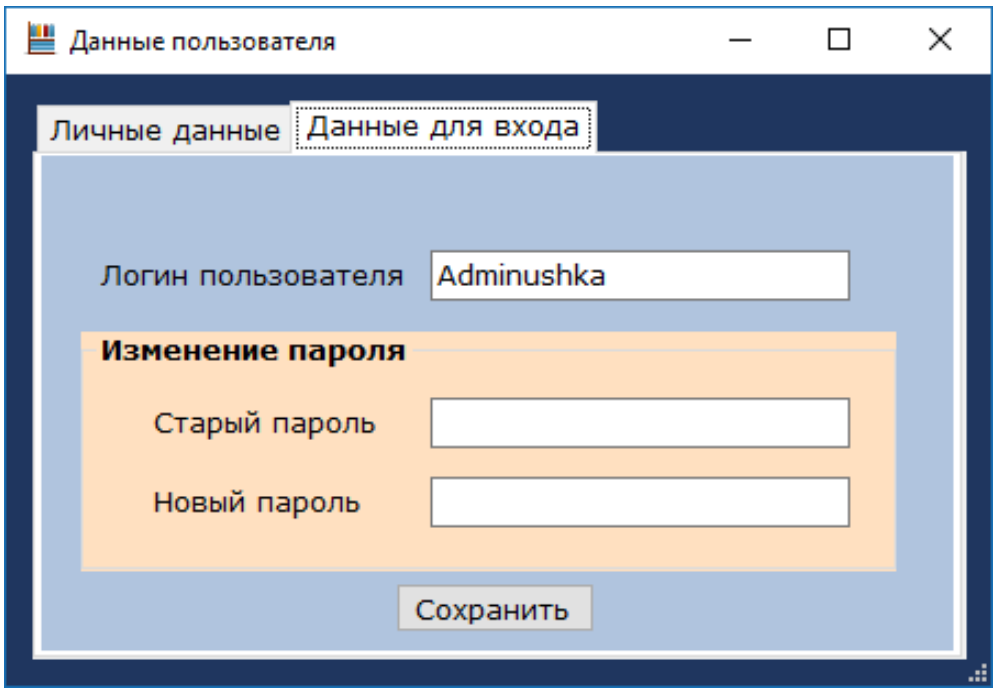

Рисунок 63 – Изменение данных пользователя

Для выхода из учётной записи необходимо нажать на имя пользователя в правом верхнем углу экрана и выбрать пункт «Выйти». После этого главная форма будет закрыта, и откроется окно авторизации.

5 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

5.1 Предмет защиты

В общем случае предмет защиты – это информация, передаваемая и хранимая в компьютерных системах в виде определённых данных, имеющих некую ценность для их владельца и потенциального нарушителя.

В случае разрабатываемой системы такими данными являются данные, хранимые в базе данных и передаваемые между клиентом и сервером.

В частности, среди таких данных, главным образом, можно выделить следующие:

- данные учётных записей пользователей (главным образом, пароль);
- личные данные работников (ФИО, должность);

Несмотря на то, что хранимые в БД личные данные работника не представляют особой ценности для злоумышленника, всё же необходимо организовать определённую защиту используемых данных (ФИО, должность), т.к. их можно отнести к персональным данным.

5.2 Угрозы ИБ

Под угрозой информационной безопасности понимают потенциальную или реальную возможность проведения случайного или преднамеренного воздействия, способного оказать определённый деструктивный эффект на защищаемую информацию.

Угрозы ИБ можно классифицировать по следующим критериям:

- аспект информационной безопасности, на который направлена угроза (конфиденциальность, целостность, доступность);
- компоненты ИС и технологии, на которые направлена угроза (программно-аппаратные комплексы, сети, поддерживающая инфраструктура и т.д.)
- способ осуществления (случайно или преднамеренно);
- локализация источника угроз (внешние и внутренние).

Учитывая, перечисленные в предыдущем пункте данные, подлежащие защите, главным образом, будут рассмотрены угрозы именно по аспекту ИБ (конфиденциальность, целостность, доступность).

Основные угрозы конфиденциальности информации:

- разглашение - сообщение или передача конфиденциальной информации лицам, не имеющим к ней допуска, в результате преднамеренных или неосторожных действий, чаще всего, сотрудников;

- утечка - бесконтрольное распространение конфиденциальной информации за пределы организации, осуществляемое по различным техническим каналам утечки информации;

- несанкционированный допуск – неправомерное преднамеренное овладение конфиденциальной информацией лицами, не имеющим к ней допуска.

Угрозы целостности:

- аппаратный сбой – кратковременный отказ или ошибка в работе аппаратных средств;

- программный сбой – нарушение работы ПО, вызванное некорректной настройкой приложения или внедрением вредоносного кода.

Угрозы доступности:

- отказ пользователей (выражается в невозможности работы с системой в силу: нежелания самого пользователя, отсутствия у пользователя подготовки, отсутствия необходимой технической поддержки);

- внутренний отказ информационной системы (возникает по причине: нарушения правил эксплуатации, ошибок в конфигурации системы, отказов ПО и АО, повреждения данных, повреждения аппаратуры;

- отказ поддерживающей инфраструктуры (нарушение работы систем связи, водоснабжения, электропитания и т.д.

5.3 Способы и средства защиты информации

Выбранные способы и средства защиты направлены, главным образом, на предотвращение угроз нарушения конфиденциальности, хранимой в базе данных информации (ФИО работника, должность, данные учётной записи).

Для обеспечения безопасности разработанной системы были использованы следующие методы и средства:

- парольная аутентификация;

- разграничение доступа;

- шифрование пароля с помощью хэш-функции SHA-512, при использовании динамической соли.

Парольная аутентификация – это проверка подлинности пользователя путём сравнения, введенного им пароля с паролем, хранящемся в базе данных и соответствующем учётной записи пользователя. Пароль – это некий набор символов, известный только пользователю, используемый для проверки подлинности пользователя. Для используемых в разработанной системе паролей было введено требование на минимальную длину, составляющую 12 символов.

Разграничение прав доступа – это процесс установления полномочий пользователя, выполняемый после аутентификации. Выделяют следующие методы разграничения доступа:

- разграничение доступа по спискам;

- использование матрицы установления полномочий;

- по уровням секретности и категориям;

- парольное разграничение доступа.

В разработанной системе используется разграничение прав доступа по категориям. Выделяется две категории пользователей: обычный пользователь и администратор. Обычный пользователь имеет доступ ко всей информации, связанной с проведением аудита безопасности: списку требований, разделов, вопросов, результатов проверок. Также он имеет возможность добавлять в список новые требования, а также проводить аудит безопасности. Администратор же, кроме информации, перечисленной выше, имеет доступ к списку пользователей системы и возможность изменять или добавлять новых пользователей в систему.

В разработанной системе хранение паролей осуществляется в зашифрованном виде, с целью предотвращения попадания их в руки злоумышленников, в случае получения последними доступа к базе данных.

Шифрование пароля выполняется путём хэширования. Хэширование – это преобразование строки данных произвольной длины в битовую строку фиксированной длины, осуществляемое по определённому алгоритму. Главная причина использования хеширования – невозможность однозначной расшифровки хэша.

Алгоритм хэширования определяется используемой хэш-функцией. В данном случае была выбрана хэш-функция SHA512, использующая 64-байтовые слова, относящаяся к семейству однонаправленных хэш-функций SHA2. Несмотря на то, что данная хэш-функция на данный момент практическая полностью неустойчива против атак удлинением сообщения, она всё ещё весьма устойчива против коллизионных атак (поиска двух различных входных блоков криптографической хеш-функции, производящих одинаковые значения хэш-функции, то есть коллизию хэш-функции). Учитывая невысокую ценность хранимой в базе данных информации, применения данной функции вполне достаточно.

Хэширование паролей происходит с применением динамической соли. Соль (в криптографии) — это случайная строка данных, передаваемая хэш-функции вместе с входным массивом данных (прообразом) для вычисления хэша (образа). Возможно использование двух типов соли: статической и динамической. Статическая соль генерируется один раз и используется для всех хэшируемых паролей, что создает определённую уязвимость, т.к. для одинаковых паролей будет генерироваться одинаковый хэш. Динамическая же соль генерируется для каждого пароля индивидуально, что что затрудняет составление словарей перебора, а также скрывает факт хранения одинаковых паролей, используемых разными пользователями. При этом стоит учитывать, что соль должна быть достаточно надёжной – иметь достаточную длину и обладать высокой энтропией (непредсказуемостью появления какого-либо символа в сообщении).

Общая схема хэширования паролей представлена на рисунке 64.

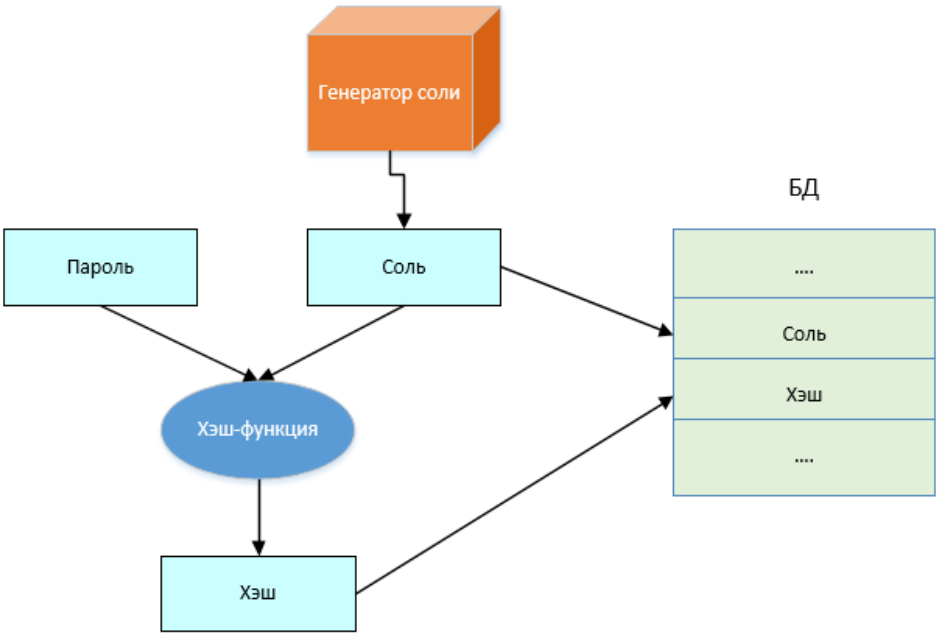

Рисунок 64 – Схема хэширования паролей

Таким образом, в базе данных осуществляется хранение не самого пароля целиком, а его хэша и значения соли. После ввода пользователем своего пароля происходит запрос к БД на получение значения соли и хэша, а затем вычисляется значение хэша для введённого пользователем пароля с использованием данной соли. Полученный хэш сравнивается с хэшем, хранимым в базе данных, и в случае, если они совпадают, введённый пароль считается верным.

6 БЕЗОПАСНОСТЬ И ЭКОЛОГИЧНОСТЬ

В данном разделе будут рассмотрены вопросы, связанные с обеспечением безопасности работника при работе с ПЭВМ, включая организацию рабочего места, правила работы с ПЭВМ, организацию графического интерфейса приложения и т.д. Также здесь будут рассмотрены вопросы экологичности и определены меры, позволяющие предотвратить чрезвычайные ситуации.

В качестве основополагающего документа будет использоваться СанПиН 2.2.2/2.4.1340-03.

6.1 Безопасность

6.1.1 Требования к ПЭВМ

Используемые ПЭВМ должны соответствовать требованиям СанПиН 2.2.2/2.4.1340-03.

Допустимые уровни электромагнитных полей (ЭМП), создаваемых ПЭВМ, также не должны превышать значений, установленных санитарно-эпидемиологическими правилами и нормативами и представленных в таблице 15.

Таблица 17 - ПДУ электромагнитных полей на рабочих местах пользователей ПК и другими средствами ИКТ

Нормируемые параметры		ПДУ
Напряженность электрического поля	5 Гц - < 2 кГц	25 В/м
	2 кГц- < 400 кГц	2,5 В/м
Напряженность магнитного поля	5 Гц- < 2 кГц	250 нТл
	2 кГц- < 400 кГц	25 нТл
Плотность потока энергии	300 МГц – 300 ГГц	10 мкВт/см^2
Напряженность электростатического поля		15 кВ/м

Концентрации вредных веществ, выделяемых ПЭВМ в воздух помещений, не должны превышать предельно допустимых концентраций (ПДК), установленных для атмосферного воздуха.

ПЭВМ должна иметь конструкцию, позволяющую выполнять поворот корпуса в горизонтальной и вертикальной плоскости, производя при этом фиксацию в заданном положении, обеспечивающую фронтальное наблюдение экрана ВДТ.

Существуют также определённые требования к дизайну ПЭВМ и периферийных устройств. Корпус ПЭВМ должен быть окрашен в спокойные мягкие тона с диффузным рассеиванием света. Клавиатура, корпус и другие блоки и устрйоства ПЭВМ должны иметь матовую поверхность с коэффициентом отражения 0,4-0,6 и не иметь блестящих деталей, способных создавать блики. Также необходимо отметить, что конструкция ВДТ должна предусматривать регулирование яркости и контрастности

6.1.2 Требования к помещениям для работы с ПЭВМ

Согласно СанПиН 2.2.2/2.4.1340-03, естественное и искусственное освещение в помещении должно соответствовать требованиям действующей нормативной документации. При этом окна в помещениях, где эксплуатируется вычислительная техника, преимущественно должны быть ориентированы на север и северо-восток. Сами оконные проемы должны быть оборудованы регулируемыми устройствами типа: жалюзи, занавесей, внешних козырьков и др.

Минимальная площадь рабочего места зависит от типа используемых мониторов (ЭЛТ или жидкокристаллические). Т.к. в организации, предположительно, используются только жидкокристаллические мониторы, то минимальная площадь рабочего места, согласно санитарным нормам, должна составлять не менее 4,5 $м^2$.

Отделка интерьера помещений, где располагаются ПЭВМ, должна быть осуществлена с использованием диффузно отражающих материалов с коэффициентом отражения для потолка - 0,7-0,8; для стен - 0,5-0,6; для пола - 0,3-0,5.

Также необходимо оборудовать помещения, используемые для размещения ПЭВМ, защитным заземлением (занулением), соответствующим техническим требованиям эксплуатации.

6.1.3 Требования к микроклимату

В помещениях, где расположены ПЭВМ, необходимо проводить ежедневную влажную уборку, а также осуществлять систематическое проветривание после каждого часа работы на ЭВМ.

Уровни положительных и отрицательных аэроионов в воздухе помещений, где расположены ПЭВМ, должны соответствовать действующим санитарно-эпидемиологическим нормативам.

Содержание вредных химических веществ в воздухе помещений, предназначенных для использования ПЭВМ не должно превышать предельно допустимых среднесуточных концентраций для атмосферного воздуха в соответствии с действующими санитарно-эпидемиологическими нормативами.

6.1.4 Требования к уровням шума и вибрации на рабочих местах, оборудованных ПЭВМ

Используемое на предприятие шумящее оборудование (серверы, печатающие устройства), уровни шума которого превышают предельно допустимые, установленные нормативами, должно быть размещено в отдельных помещениях.

Предельно допустимые уровни звука на рабочих местах для трудовой деятельности разных категорий определяются СанПиН 2.2.4.3359-16 "Санитарно-эпидемиологические требования к физическим факторам на рабочих местах".

Таблица 18 - Эквивалентные уровни звука на рабочих местах для трудовой деятельности разных категорий напряженности и тяжести, дБА

Предельно допустимые эквивалентные уровни звука, дБА			
Категории тяжести трудового процесса	Категории тяжести трудового процесса		
	легкая и средняя физическая нагрузка	тяжелый труд 1 степени	тяжелый труд 2 степени
Напряженность легкой и средней степени	80	75	75
Напряженный труд 1 степени	70	65	65
Напряженный труд 2 степени	60	-	-
Напряженный труд 3 степени	50	-	-

6.1.5 Требования к освещению на рабочих местах, оборудованных ПЭВМ

Рабочие столы должны быть размещены таким образом, чтобы видеодисплейные терминалы были ориентированы боковой стороной к световым проемам. Необходимо это для того, чтобы естественный свет падал, главным образом, с левой стороны.

В качестве искусственного освещения в помещениях для работы с ПЭВМ должна применяться система общего равномерного освещения. В случае преимущественной работы с документами необходимо применять системы комбинированного освещения.

Освещенность на поверхности стола в зоне размещения рабочего документа должна быть 300-500 лк. Освещение не должно создавать бликов на поверхности экрана. Освещенность поверхности экрана не должна быть более 300 лк.

6.1.6 Требования к визуальным параметрам ВДТ, контролируемым на рабочих местах

Предельно допустимые значения визуальных параметров ВДТ, контролируемые на рабочих местах, определяются СанПиН 2.2.2/2.4.1340-03.

Таблица 19 - Визуальные параметры ВДТ, контролируемые на рабочих местах

№	Параметры	Допустимые значения
1	Яркость белого поля	Не менее 35 кд/кв.м
2	Неравномерность яркости рабочего поля	Не более +-20%
3	Контрастность (для монохромного режима)	Не менее 3:1
4	Временная нестабильность изображения (мелькания)	Не должна фиксироваться
5	Пространственная нестабильность изображения (дрожание)	Не более 2 x 10(-4L), где L - проектное расстояние наблюдения, мм

6.1.7 Общие требования к организации рабочих мест пользователей ПЭВМ

Размещать рабочие места с ПЭВМ нужно таким образом, чтобы расстояние между рабочими столами с мониторами (в направлении тыла поверхности одного видеомонитора и экрана другого видеомонитора) составляло не менее двух метров, а расстояние между боковыми поверхностями видеомониторов - не менее 1,2 м.

Экран монитора должен располагаться на расстоянии 600-700 мм от глаз пользователя. При этом данное расстояние не должно быть меньше 500 мм с учетом размеров алфавитно-цифровых знаков и символов.

Рабочий стол должен иметь такую конструкцию, которая могла бы обеспечить оптимальное размещение на рабочей поверхности используемого оборудования с учетом его количества и конструктивных особенностей, характера выполняемой работы. Поверхность рабочего стола должна иметь коэффициент отражения 0,5-0,7.

Конструкция рабочего стула (кресла) должна обеспечивать поддержание рациональной рабочей позы при работе на ПЭВМ, позволять изменять позу с целью снижения статического напряжения мышц шейно-плечевой области и спины для предупреждения развития утомления. Тип рабочего стула (кресла) следует выбирать с учетом роста пользователя, характера и продолжительности работы с ПЭВМ.

Рабочий стул (кресло) должен быть подъемно-поворотным, регулируемым по высоте и углам наклона сиденья и спинки, а также расстоянию спинки от переднего края сиденья, при этом регулировка каждого параметра должна быть независимой, легко осуществляемой и иметь надежную фиксацию.

Поверхность сиденья, спинки и других элементов стула (кресла) должна быть полумягкой, с нескользящим, слабо электризующимся и воздухопроницаемым покрытием, обеспечивающим легкую очистку от загрязнений.

6.1.8 Требования к организации и оборудованию рабочих мест с ПЭВМ для взрослых пользователей

Высота рабочей поверхности стола для взрослых пользователей должна регулироваться в пределах 680-800 мм; при отсутствии такой возможности высота рабочей поверхности стола должна составлять 725 мм.

Модульными размерами рабочей поверхности стола для ПЭВМ, на основании которых должны рассчитываться конструктивные размеры, следует считать: ширину 800, 1000, 1200 и 1400 мм, глубину 800 и 1000 мм при нерегулируемой его высоте, равной 725 мм.

Рабочий стол должен иметь пространство для ног высотой не менее 600 мм, шириной - не менее 500 мм, глубиной на уровне колен - не менее 450 мм и на уровне вытянутых ног - не менее 650 мм.

Конструкция рабочего стула должна обеспечивать:

- ширину и глубину поверхности сиденья не менее 400 мм;

- поверхность сиденья с закругленным передним краем;

- регулировку высоты поверхности сиденья в пределах 400-550 мм и углам наклона вперед до 15° и назад до 5°;

- высоту опорной поверхности спинки 300±20 мм, ширину - не менее 380 мм и радиус кривизны горизонтальной плоскости - 400 мм;

- угол наклона спинки в вертикальной плоскости в пределах ±30°;

- регулировку расстояния спинки от переднего края сиденья в пределах 260-400 мм;

- стационарные или съемные подлокотники длиной не менее 250 мм и шириной - 50-70 мм;

- регулировку подлокотников по высоте над сиденьем в пределах 230±30 мм и внутреннего расстояния между подлокотниками в пределах 350-500 мм.

Рабочее место пользователя ПЭВМ следует оборудовать подставкой для ног, имеющей ширину не менее 300 мм, глубину не менее 400 мм, регулировку

по высоте в пределах до 150 мм и по углу наклона опорной поверхности подставки до 20°. Поверхность подставки должна быть рифленой и иметь по переднему краю бортик высотой 10 мм.

Клавиатуру следует располагать на поверхности стола на расстоянии 100-300 мм от края, обращенного к пользователю, или на специальной, регулируемой по высоте рабочей поверхности, отделенной от основной столешницы.

6.1.9 Организация интерфейса программы

Стандарт ГОСТ Р ИСО 6385—2016 – «Применение эргономических принципов при проектировании производственных систем» определяет базовую структуру учета принципов эргономики при проектировании производственных систем и анализе производственных ситуаций. Положения настоящего стандарта применимы также к проектированию и разработке продукции.

Интерфейс любого программного приложения должен обеспечивать взаимодействие между пользователем и техническим оборудованием.

Интерфейс разработанного приложения соответствует следующим принципам:

- прозрачность (простота освоения);
- общее стилевое оформление;
- использование графической информации;
- использование адекватного сочетания цветов.

6.2 Экологичность

Основные вопросы, связанные с обеспечением экологичности в процессе осуществления предприятием своей деятельности, регламентируются Федеральным законом "Об отходах производства и потребления" от 24.06.1998 N 89-ФЗ. Данный закон определяет правила и порядок обращения с отходами производства и потребления, включая их утилизацию в целях предотвращения вредного воздействия их на окружающую среду и здоровье человека.

Статья 4.1 – Классы опасности отходов классифицирует отходы в зависимости от степени их вредного воздействия на окружающую среду, выделяя пять классов опасности:

- 1 класс - чрезвычайно опасные отходы;

- 2 класс - высокоопасные отходы;

- 3 класс - умеренно опасные отходы;

- 4 класс - малоопасные отходы;

- 5 класс - практически неопасные отходы.

Бумажные отходы должны передаваться в пункт приёма макулатуры. На территории Благовещенска существует компания ОАО "ВТОРРЕСУРСЫ", куда могут быть переданы отходы этого типа.

Пластиковые отходы должны быть утилизированы в специальных урнах для пластиковых отходов.

Утилизация оргтехники и компьютерной техники, согласно российскому законодательству, является обязательным не только для организаций, но и для физических лиц. При этом утилизацию должны проводить специализированные предприятия, имеющие соответствующую лицензию. Связано это всё, главным образом, с тем, что внутри микросхем и плат технических устройств находятся компоненты, содержащие определённую долю драгоценных металлов. Согласно законодательству РФ, любые организации должны вести учет драгоценностей в составе собственных основных средств. Одной из таких компаний, занимающейся утилизацией оргтехники и компьютеров на территории Благовещенска, является ФПК-Сервис.

6.3 Пожарная безопасность

Согласно НПБ 105-03, помещения, используемые для эксплуатации ЭВМ, можно отнести к категории В – пожароопасные помещения. Поэтому в данном случае весьма важным является обеспечение пожарной безопасности.

Во-первых, на предприятии должен быть составлен план эвакуации. При этом при его оформлении, согласно ГОСТ 12.4.026-2015, должны использоваться сигнальные цвета.

Во-вторых, предприятие должно быть оснащено первичными средствами пожаротушения, такими как огнетушители. В соответствии с СП 9.13130.2009,

огнетушители должны размещаться таким образом, чтобы расстояние от возможного очага пожара до ближайшего огнетушителя не превышало 20 м, а на каждом этаже было не менее двух огнетушителей. При этом необходимо помнить, что один раз в квартал происходит внешний осмотр огнетушителей, а перезарядка огнетушителей выполняется один раз в пять лет.

В-третьих, предприятие должно иметь эвакуационный выход. Согласно СП 1.13130.2009, высота эвакуационных выходов в свету должна быть не менее 1,9 м, ширина выходов в свету - не менее 0,8 м, за исключением специально оговоренных случаев.

В-четвёртых, на предприятии должны быть установлена пожарная сигнализация для оповещения персонала.

6.4 Комплексы физических упражнений для сохранения и укрепления индивидуального здоровья и обеспечения полноценной профессиональной деятельности

6.4.1 Комплексы упражнений для глаз

В приложении 8 к СанПиНу 2.2.2/2.4.1340-03 представлено три различных комплекса упражнений для глаз, рекомендуемых работающим за ПК. Ниже будет описан один из таких комплексов.

Приведённые ниже упражнения выполняются сидя или стоя, отвернувшись от экрана, при ритмичном дыхании, с максимальной амплитудой движения глаз.

Список упражнений:

1. Закрыть глаза, сильно напрягая глазные мышцы, на счет 1-4, затем раскрыть глаза, расслабив мышцы глаз, посмотреть вдаль на счет 1 -6. Повторить 4 -5 раз.2.

2. Посмотреть на переносицу и задержать взор на счет 1 -4. До усталости глаза не доводить. Затем открыть глаза, посмотреть вдаль на счет 1 -6. Повторить 4 -5 раз.

3. Не поворачивая головы, посмотреть направо и зафиксировать взгляд на счет 1 -4, затем посмотреть вдаль прямо на счет 1-6. Аналогичным образом проводятся упражнения, но с фиксацией взгляда влево, вверх и вниз. Повторить 3 - 4 раза.

4. Перевести взгляд быстро по диагонали: направо вверх -налево вниз, потом прямо вдаль на счет 1 -6; затем налево вверх направо вниз и посмотреть вдаль на счет 1 -6. Повторить 4 -5раз.

6.4.2 Комплексы физических упражнений

Комплексы физических упражнений, ориентированные на людей, занимающихся сидячей работой, включая работу за ПК, направлены на снятие локального утомления и предназначены для чётко определённого воздействия на ту или иную группу мышц.

В приложении 9 к СанПиНу 2.2.2/2.4.1340-03 также описано четыре различных комплекса физических упражнений общего назначения, рекомендуемых работающим за ПК. Ниже будет описан один из таких комплексов.

Список упражнений:

1. Исходное положение -о.с. 1 -2 -встать на носки, руки вверх-наружу, потянуться вверх за руками.3 -4 -дугами в стороны руки вниз и расслабленно скрестить перед грудью, голову наклонить вперед. Повторить 6 -8 раз. Темп быстрый.

2. Исходное положение - стойка ноги врозь, руки вперед, 1 -поворот туловища направо, мах левой рукой вправо, правой назад за спину. 2 и.п. 3 -4 -то же в другую сторону. Упражнения выполняются размашисто, динамично. Повторить 6 -8 раз. Темп быстрый.

3. Исходное положение 1 -согнуть правую ногу вперед и, обхватив голень руками, притянуть ногу к животу. 2 -приставить ногу, руки вверх-наружу. 3 -4 -то же другой ногой. Повторить 6 -8 раз. Темп средний.

ЗАКЛЮЧЕНИЕ

В ходе выполнения работы была проведена разработка автоматизированной системы для аудита политики информационной безопасности на соответствие ГОСТ.

В целом, работа выполнялась в несколько этапов.

Во-первых, был произведён анализ предметной области, в ходе которого были рассмотрены такие понятия, как информационная безопасность и требования к ИБ, политика безопасности, оценка рисков и способы такой оценки и т.д.

Во-вторых, были проведены все этапы проектирования системы, включая:

- обоснование необходимости разработки;
- выбор среды разработки;
- описание функциональных и обеспечивающих подсистем;
- проектирование БД.

В-третьих, была произведена непосредственно разработка самого программного приложения.

Результатом выполнения всех вышеперечисленных этапов стала разработанная автоматизированная система, позволяющая проводить проверку политики безопасности на соответствие требованиям стандарту ГОСТ либо требованиям, добавленным самими пользователями, а также вычислять значение и степень риска ИБ и анализировать его распределение по тестируемым разделам ИБ.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1 Методические указания к выполнению и защите выпускной квалификационной работы бакалавра / [ред. С.Г. Самохвалова]. – Благовещенск: АмГУ, 2017. – 50с.

2 Грофф, Д.: SQL. Полное руководство: учебное пособие / Д. Грофф, П. Вайнберг. - СПб.: Вильямс, 2016, 960 с.

3 Троелсен, Э.: Язык программирования C# 7 и платформы .NET и .NET Core, 8-е изд. : Пер. с англ. — СПб. : ООО “Диалектика”, 2018 — 1328 с.

4 Коннопли, Т.: Базы данных. Проектирование, реализация и сопровождение. Теория и практика: учебное пособие / Т. Коннопли, К. Бегг.– 3-е издание. – СПб.: Вильямс, 2017. – 1440 с.

5 Королёв, В.Т.: Технология ведения баз данных [Электронный ресурс]: учебное пособие/ Королёв В.Т., Контарёв Е.А., Черных А.М.— Электрон. текстовые данные.— М.: Российский государственный университет правосудия, 2015.— 108 с.— Режим доступа: http://www.iprbookshop.ru/45233.— ЭБС «IPRbooks», по паролю

6 Петренко, С. А.: Политики информационной безопасности / С. А. Петренко, В. А. Курбатов. – М. : Компания АйТи, 2006. – 400 с

7 Нестеров, С.А. Основы информационной безопасности: Учебное пособие.— 2-е изд., стер. — СПб.: Издательство «Лань», 2016. — 324 с.— (Учебники для вузов. Специальная литература).

8 Бирюков, А.А.: Информационная безопасность: защита и нападение. - М.: ДМК Пресс, 2012. - 474 с.: ил.

9 Туманов, В.Е. Основы проектирования реляционных баз данных / В.Е. Туманов. – М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. – 502 с.

10 Автоматизированные информационные системы: учебник для студ. учреждений сред. проф. образования / К.Н.Мезенцев. − 4-е изд., стер. − М. : Издательский центр «Академия», 2013. − 176 с.

11 Маглинец, Ю.А. Анализ требований к автоматизированным информационным системам. М. Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. – 191 с.

12 Кумскова, И.А. Базы данных: учеб. Пособие / И.А. Кумскова. – 3-е издание. – М.: Изд-во КноРус, 2016 год. – 488 с.

13 ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности. - утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 24 сентября 2012 г. N 423-ст.

14 ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. - утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 18 декабря 2008 г. N 532-ст.

15 ГОСТ Р ИСО/МЭК 27005-2010 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности - утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 30 ноября 2010 г. N 632-ст

16 ГОСТ Р ИСО 6385—2016 Применение эргономических принципов при проектировании производственных систем - утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 20 октября 2016 г. N 1445-ст

17 Санитарно-эпидемиологические правила и нормативы. СанПиН 2.2.2/2.4.1340-03. Гигиенические требования к персональным электронно-вычислительным машинам и организации работы.

18 Санитарно-эпидемиологические правила и нормативы. СанПиН 2.2.4.3359-16. Санитарно-эпидемиологические требования к физическим факторам на рабочих местах

ПРИЛОЖЕНИЕ А

Функциональная модель системы

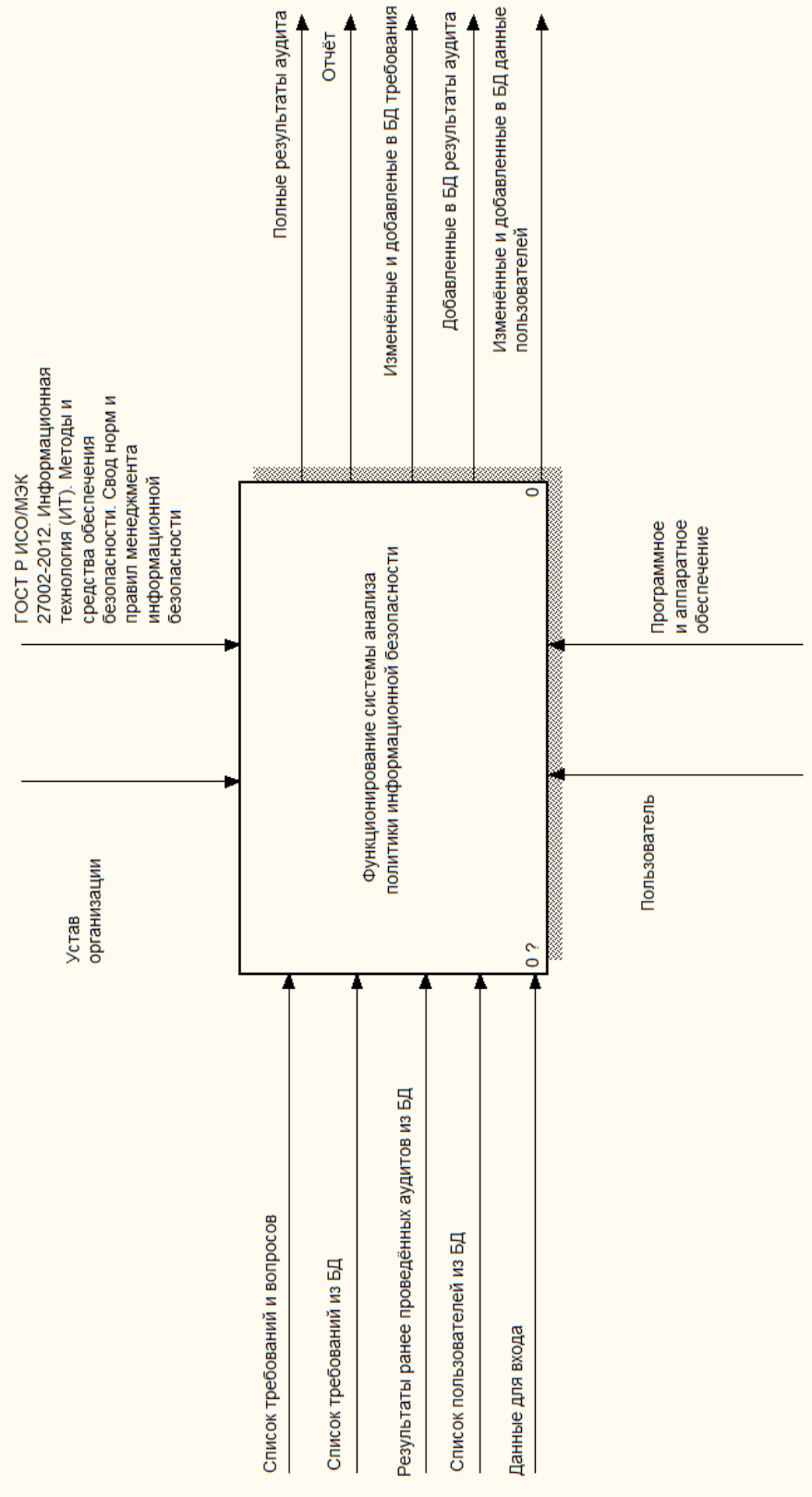

Рисунок А.1 – Контекстная диаграмма

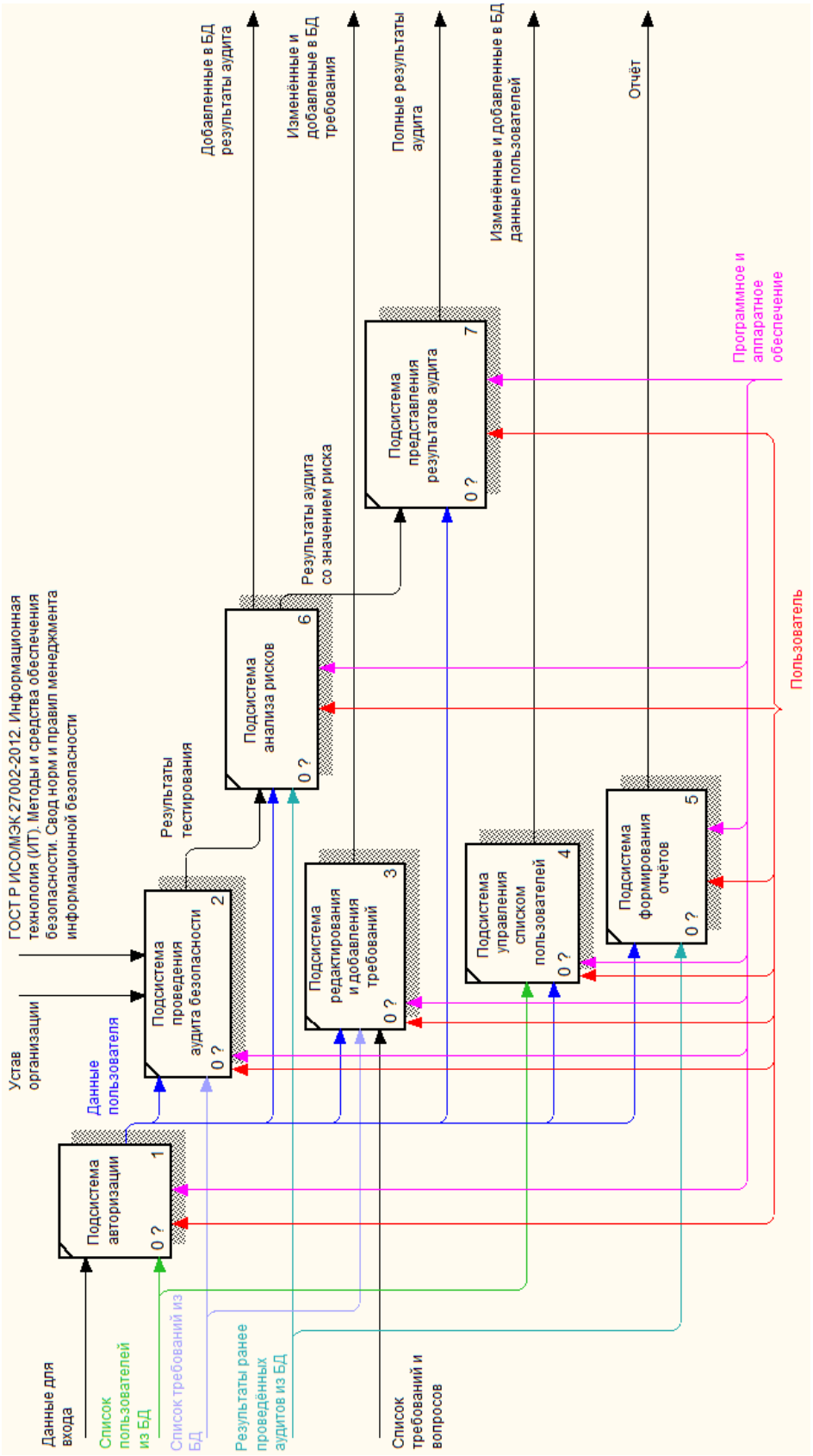

Рисунок А.2 – Декомпозиция контекстной диаграммы

ПРИЛОЖЕНИЕ Б

Техническое задание

1 ОБЩИЕ СВЕДЕНИЯ

1.1 Полное название системы

Автоматизированная система «Аудит политики безопасности»

1.2 Наименование разработчика

Разработчик: студент 655-об группы факультета математики и ин-форматики Амурского государственного университета Копылов Никита Юрьевич.

1.3 Плановые сроки начала и окончания работы

Срок начала работ: 01 апреля 2020 г.

Срок окончания работ: 30 июня 2020 г.

2 НАЗНАЧЕНИЕ И ЦЕЛИ СОЗДАНИЯ СИСТЕМЫ

2.1 Назначение системы

Разрабатываемая автоматизированная система предназначена для решения следующих задач:

- автоматизированное проведение аудита информационной безопасности;
- хранение результатов аудитов в БД;
- осуществление анализа рисков ИБ;
- проверка соответствия существующей политики безопасности на соответствие стандарту ГОСТ Р ИСО/МЭК 27002-2012.

2.2 Цели создания системы

- автоматизация процесса проведения аудита информационной безопасности;
- повышение эффективности анализа рисков.

Продолжение ПРИЛОЖЕНИЯ Б

3 ХАРАКТЕРИСТИКА ОБЪЕКТОВ АВТОМАТИЗАЦИИ

3.1 Краткие сведения об объекте автоматизации

Объектом автоматизации является процесс проведения аудита политики безопасности.

3.2 Сведения об условиях эксплуатации и о характеристике окружающей среды.

Для того чтобы начать работать с программой вначале необходимо осуществить установку локального сервера БД MAMP, а затем в приложении phpMyAdmin экспортировать приложенную к системе базу данных. Подробная информация по установке сервера и эксплуатации программы указана в прилагающейся к изделию документации.

4 ТРЕБОВАНИЯ К СИСТЕМЕ

4.1 Требования к системе в целом

4.1.1 Требования к структуре и функционированию системы

Разрабатываемая система должна быть централизованной, то есть все данные должны располагаться в центральном хранилище.

В системе выделяются следующие функциональные подсистемы:

- подсистема проведения аудита безопасности;
- подсистема редактирования и добавления требований;
- подсистема представления результатов аудита;
- подсистема анализа рисков.

4.1.2 Требования к надежности

К разрабатываемой системы предъявляются следующие требования по надёжности:

- устойчивость к аппаратным сбоям;
- устойчивость к программным сбоям;
- защищённость от выполнения пользователями неверных действий;

Выполнение предъявляемых к надёжности требований должно обеспечиваться путём проведения следующих организационных мероприятий:

- назначения администратора БД для установления над ней контроля в целях предотвращения её искажения;

- выполнение предварительного обучения пользователей;

- соблюдение правил эксплуатации аппаратных средств;

- соблюдение правил эксплуатации общесистемного ПО;

- своевременное выполнение процедур резервного копирования данных.

4.1.3 Требования к интерфейсу

Интерфейс разрабатываемой системы должен удовлетворять следующим требованиям:

- быть интуитивно понятным;

- иметь адекватную цветовую гамму, не затрудняющую чтение текста;

- иметь определённые графические средства, облегчающие выполнение пользователем тех или иных функций.

4.1.3 Требования к безопасности

К разрабатываемой системе предъявляются следующие требования безопасности:

- отслеживание ошибок ввода данных;

- отслеживание умышленного искажения данных;

- отслеживание внедрения в программный код вредоносного кода.

4.2 Требования к функциям

Разрабатываемая система должна поддерживать выполнение следующих функций:

- проведение аудита безопасности в виде теста;

- возможность добавления пользователем новых разделов, требований и вопросов;

- возможность удаления добавленных ранее пользователем требований;

- возможность просмотра результатов проведённых тестов;
- возможность просмотра значений рисков по каждому аудиту.

4.3 Требования к видам обеспечения

4.3.1 Требования к лингвистическому обеспечению

Для разработки автоматизированной системы должна быть использована среда визуального программирования Microsoft Visual Studio 2019 с использованием языка C#. База данных должна быть разработана с использованием языка SQL.

4.3.3 Требования к программно-аппаратному обеспечению

Техническое обеспечение включает в себя комплекс технических средств, используемых для работы автоматизированной системы.

Минимальные технические характеристики ПК клиента:

- тактовая частота процессора не ниже 1,8 ГГц;
- 2 ГБ ОЗУ;
- 800 Мб на жёстком диске;

Минимальные технические характеристики ПК сервера:

- тактовая частота процессора не ниже 3 ГГц;
- 4 ГБ ОЗУ;
- жёсткий диск объёмом 500 Гб;

Программное обеспечение включает комплекс программ, необходимых для нормальной работы разрабатываемой системы, а также обеспечивающих функционирование комплекса технических средств.

На сервере может быть установлена одна из перечисленных ОС семейства Windows: Windows 7, Windows 8.1, Windows 10. В качестве локальной серверной среды должна быть установлена MAMP.

4.3.4 Требования к математическому обеспечению

Сложное математическое обеспечение не требуется

4.3.5 Требования к документированию

Документация к проекту должна включать следующие документы:

- Техническое задание (ТЗ);
- Описание базы данных (БД);
- Описание разработанного программного обеспечения;
- Руководство пользователя.

4.3.6 Требования к эксплуатации

Работа с клиентским приложением системы должна требовать минимальной предварительной подготовки персонала.

5 СОСТАВ И СОДЕРЖАНИЕ РАБОТ ПО СОЗДАНИЮ СИСТЕМЫ

5.1 Перечень стадий и этапов работ по созданию системы

Процесс создания системы включает следующие этапы:

1 этап - проведение анализа предметной области, выделение объекта автоматизации;

2 этап - составление технического задания, включает:

- выявление требований к разрабатываемой системе,
- формирование перечня необходимых программных и аппаратных средств для реализации проекта,
- уточнение функций системы;

3 этап – проектирование БД, включает:

- инфологическое проектирование,
- логическое проектирование,
- физическое проектирование;

4 этап – проектирование программного приложения:

- выделение функциональных подсистем,
- разработка иерархии функциональных подсистем в соответствии с ООП,
- выделение подсистемы обеспечения информационной безопасности,
- обоснование выбора программных платформ разработки и дизайна, а также языков программирования,

- разработка документации, связанной с рассмотрением аспектов безопасности жизнедеятельности,

- выделение задач функциональных подсистем;

5 этап - программная реализация системы, включает написание кода и тестирование;

6 этап - согласование созданной информационной системы с поставленными требованиями;

7 этап - внедрение и сопровождение подсистемы: установка и настройка программно-аппаратных средств, обучение пользователей работе с программно-аппаратным комплексом.

6 ПОРЯДОК КОНТРОЛЯ И ПРИЕМКИ ПАК

Контроль и приёмка разработанного ПАК будет осуществляться поэтапно в соответствии с календарным планом.

Список этапов:

- анализ готовой систем;

- проверка разработанной системы на соответствие техническому заданию, с целью определения, выполнены ли все требования;

- выполнение доработки и изменений системы при необходимости;

–опытная эксплуатация системы в режиме бета-тестирования;

– доработка системы и исправление ошибок.

Приёмка работ осуществляется заказчиком.

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

Перед началом эксплуатации разработанного программного продукта необходимо провести следующий перечень работ:

- определить лиц, ответственных за процесс внедрения ПАК в эксплуатацию;

- провести обучение пользователей;

- обеспечить соответствие помещений и рабочих мест пользователей системы требованиям, определённым ТЗ;

- обеспечить выполнение всех требований к программным и аппаратным средствам, на которых основывается работа разработанной системы;

- провести опытную эксплуатацию АС.

8 ТРЕБОВАНИЯ К ДОКУМЕНТИРОВАНИЮ

8.1 Перечень подлежащих обработке документов

При сдаче системы в эксплуатацию должен быть подготовлен и передан заказчику следующий перечень документов:

– техническое задание;

– описание программного продукта;

- руководство пользователя

8.2. Перечень документов на машинных носителях

Вся представленная в подразделе 8.1 документация должна быть представлена на машинных носителях

Документация из подраздела 8.1 должна быть представлена на машинных носителях.