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 Информационные системы и технологии

ДОПУСТИТЬ К ЗАЩИТЕ
Зав. кафедрой
_____А.В. Бушманов
«_____»_____2023г.

БАКАЛАВРСКАЯ РАБОТА

на тему: Разработка ИС оценки уровня благонадежности соискателя на должность специалиста по защите информации

Исполнитель
студент группы 955-об _____ (подпись, дата) Д.В. Панасюк

Руководитель
доцент, канд. техн. наук _____ (подпись, дата) Л.В. Никифорова

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

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

Благовещенск 2023

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

Факультет математики и информатики
Кафедра информационных и управляющих систем

УТВЕРЖДАЮ
Зав. кафедрой
_____ А.В. Бушманов
«_____»_____2023г,

ЗАДАНИЕ

К выпускной квалификационной работе студента: Панасюк Дарьи Владимировны

1. Тема выпускной квалификационной работы: Разработка ИС оценки уровня благонадежности соискателя на должность специалиста по защите информации

(Утверждена приказом от_____№_____)

2. Срок сдачи студентом законченной работы (проекта): 20.06.2023

3. Исходные данные к выпускной квалификационной работе: техническое задание на разработку ИС, нормативная документация, специальная литература

4. Содержание выпускной квалификационной работы (перечень подлежащих разработке вопросов): анализ ПрО, разработка методологии оценки уровня благонадежности, проектирование ИС, реализация ИС, анализ инструментальных средств разработки, выбор средств разработки

5. Перечень материалов приложения: техническое задание на разработку ИС, пример тестовых и кейс-тестовых заданий, перечень анкетных вопросов

6. Консультанты по выпускной квалификационной работе: по безопасности и экологичности – Булгаков А. Б., доцент, канд. техн. наук

7. Дата выдачи задания: 01.10.2022

Руководитель выпускной квалификационной работы: Никифорова Лариса Владимировна, доцент, канд. техн. наук _____

Задание принял к исполнению (01.10.2022): _____

РЕФЕРАТ

Бакалаврская работа содержит 80 страниц, 31 рисунок, 25 источников, 8 таблиц, 4 приложения

ИНФОРМАЦИОННАЯ СИСТЕМА, БАЗА ДАННЫХ, СИСТЕМА ПРИНЯТИЯ РЕШЕНИЙ, БЛАГОНАДЕЖНОСТЬ, СОИСКАТЕЛЬ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ, МЕТОДОЛОГИЯ, ТЕСТИРОВАНИЕ

Объект исследования: процесс оценки уровня благонадежности.

Цель данной выпускной квалификационной работы заключается в разработке инструмента для подбора благонадежного персонала, способного обеспечить безопасность информации в организации, для этого предлагается создать автоматизированную информационную систему, которая позволит проводить оценку кандидатов на соответствие профессиональным и личностным компетенциям.

Для достижения цели были задействованы следующие методы:

– *анализ*: проведение исследования предметной области, изучение профессионального стандарта специалиста по защите информации № 06.033, кластеризация понятия благонадежности;

– *формализация*: превращает понятие «Благонадежность соискателя» в число, выражающее процентное представление между рекомендуемым и фактическим уровнем благонадежности;

– а*налогия*: использование сравнительного анализа для выявления наиболее эффективных подходов оценки уровня благонадежности;

– *синтез*: создание комплексной модели оценки уровня благонадежности соискателя, объединяющей профессиональные и личностные качества;

– *измерение*: количественная оценка уровня благонадежности с помощью различных метрик.

В результате работы была разработана АИС, способная эффективно оценивать уровень благонадежности соискателей на должность специалиста по защите информации. Эта система основана на современных методах анализа данных и использует комплексный подход, который объединяет профессиональные и личностные компетенции кандидатов. Результаты оценки представлены в виде метрик, которые обеспечивают высокую точность и достоверность информации, необходимой для принятия решений о найме соискателей.

Данная работа может быть использована рекрутерами, HR-специалистами и руководителями организаций при подборе персонала на должности, связанные с защитой информации.

Область применения ИС оценки уровня благонадежности соискателей может быть широкой и включает в себя различные сферы бизнеса, такие как финансовый, медицинский, государственный и другие секторы, где защита информации является ключевым аспектом деятельности.

НОРМАТИВНЫЕ ССЫЛКИ

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

ГОСТ 19. 001-77. Единая система программной документации (ЕСПД). Общие положения.

ГОСТ 19. 002-80. ЕСПД. Схемы алгоритмов и программ. Правила выполнения.

ГОСТ 19. 003-80. ЕСПД. Схемы алгоритмов и программ. Обозначения условные графические.

ГОСТ 19. 004-80. ЕСПД. Термины и определения.

ГОСТ 19. 101-77. ЕСПД. Виды программ и программных документов.

ГОСТ 19. 102-77. ЕСПД. Стадии разработки.

ГОСТ 19. 201-78. ЕСПД. Техническое задание. Требования к содержанию и оформлению.

ГОСТ 19. 301-79. ЕСПД. Программа и методика испытаний. Требования к содержанию и оформлению.

ГОСТ 19. 402-78. ЕСПД. Описание программы.

ГОСТ 19. 502-78. ЕСПД. Описание применения.

ГОСТ 2. 701-84. Схемы. Типы и виды. Общие требования к выполнению.

ГОСТ 19. 701-90. Схемы алгоритмов, программ, данных и систем.

ГОСТ 19. 102-77. Стадии разработки.

ГОСТ 19. 404-79. Пояснительная записка. Требования к содержанию и оформлению.

ГОСТ Р 53891-2010 Информационные технологии. Средства защиты информации. Классификация и общие требования.

ГОСТ Р ИСО/МЭК 27005 Информационная технология. Методы обеспечения информационной безопасности. Менеджмент риска информационной безопасности.

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

АИС	автоматизированная информационная система
ИС	информационная система
СУБД	система управления базами данных
БД	база данных
ИБ	информационная безопасность
ОС	операционная система
ПО	программное обеспеченье
ГУМВД	Главное управление Министерства внутренних дел
ЦИТ и ЗИ	центр информационных технологий, связи и защиты информации
ЧС	чрезвычайная ситуация

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Тема благонадежности сотрудников является активно развивающейся областью, особенно в свете быстро меняющейся ситуации в мире информационных технологий и компьютерной безопасности.

Существует множество научных работ и практических решений, направленных на повышение уровня благонадежности сотрудников. Например, разработаны методы оценки профессиональных качеств кандидатов на должность, включая проверку знаний, навыков и опыта работы. Также разрабатываются и внедряются в организации системы контроля доступа к информации, анализа логов и мониторинга активности сотрудников для выявления подозрительных действий.

Однако, существующие методы не всегда являются эффективными и не всегда могут гарантировать полную благонадежность сотрудников. В связи с этим, в настоящее время активно идет работа над разработкой новых подходов и технологий, включая использование машинного обучения, искусственного интеллекта и биометрических технологий.

Таким образом, можно сделать вывод, что современное научно-техническое состояние по теме благонадежности сотрудников является динамичным и перспективным, однако требует дальнейшего развития и совершенствования методов и технологий.

Для проведения исследования необходимо использовать следующие исходные данные:

– информация о существующих системах оценки благонадежности кандидатов;

– данные об уровне знаний и навыков, необходимых для работы в области защиты информации;

– данные о конкретных проблемах, которыми обладают специалисты по защите информации;

– данные об актуальных требованиях к должностям в области защиты информации.

Эти сведения позволят провести комплексное и качественное исследование, а также разработать эффективную систему оценки благонадежности соискателей на должность специалиста по защите информации.

Актуальность: исходя из увеличения угроз информационной безопасности, таких как DDoS-атаки, фишинг, компрометация учетных записей, а также с учетом серьезных утечек конфиденциальных данных, таких как случаи с «Дикси», Best2pay и «Яндекс», становится ясно, что защита данных является ключевой задачей для компаний и организаций. Разработка системы оценки уровня благонадежности соискателей на должность специалиста по защите информации становится необходимой мерой для предотвращения утечек данных и обеспечения информационной безопасности предприятия.

Научная новизна проекта заключается в том, что ранее не было разработано системы оценки уровня благонадежности соискателя на должность специалиста по защите информации, которая была бы основана на комплексном анализе знаний и навыков кандидата в данной области, а также учитывала бы не только профессиональные данные, но и личностные характеристики кандидатов, такие как их предрасположенность к честности и ответственности, склонность к лжи и т.д.

Практическая значимость исследования заключается в разработке программного продукта для обеспечения кадровой безопасности предприятия путем правильно подобранных благонадежных кадров, обладающих требуемыми компетенциями, навыками и высокими нравственными устоями. Разработанный сервис позволит оценить уровень соискателя, не прибегая к дополнительным параметрам и методам оценки уровня благонадежности, так как будет содержать исключительно вопросы и задания по ключевым темам описанных в профессиональном стандарте, что способствует отсеиванию

лишних вопросов к кандидату и устранению сомнений в его компетенциях на претендуемую должность.

Связь данного исследования с другими, ранее проведенными работами заключается в том, что оно продолжает тему оценки кандидатов на должность в целом, однако в данном случае уделено особое внимание специалистам по защите информации и оценке их уровня знаний и навыков в данной области. Также, данное исследование может быть использовано в дальнейшем для развития более сложных систем оценки благонадежности соискателей на различные должности.

Целью данной работы является разработка информационной системы оценки уровня благонадежности соискателя на должность специалиста по защите информации, которая позволит эффективно оценивать уровень знаний, навыков и моральной нравственности кандидата, а также повышать показатель безопасности данных в организации.

1 АНАЛИЗ ПРЕДМЕТНОЙ ОБЛАСТИ

1.1 Организация: обзор и особенности

1.1.1 ГУМВД

Главное управление Министерства внутренних дел России (ГУМВД) по Амурской области является ключевым органом исполнительной власти, ответственным за поддержание правопорядка и обеспечение общественной безопасности на территории Амурской области.

Местонахождение ГУМВД: 50 лет Октября 18, г. Благовещенск, 675000.

Предметная область ГУМВД содержит широкий спектр задач и функций, включая:

– охрану общественного порядка: ГУМВД реализует меры по поддержанию общественного порядка, предотвращению противоправных действий и обеспечению безопасности граждан;

– борьбу с преступностью: основной задачей ГУМВД является предотвращение, выявление и расследование преступлений различной категории, включая кражи, грабежи, наркотическую и экономическую преступность, преступления против личности и имущества;

– охрану государственной тайны: ГУМВД выполняет функции по обеспечению охраны государственной тайны в соответствии с действующим законодательством;

– безопасность на дорогах: организация контроля за дорожным движением, предотвращение нарушений ПДД, расследование ДТП и пресечение преступлений, связанных с дорожным движением, также входят в обязанности ГУМВД;

– борьбу с киберпреступностью: в современной информационной эпохе ГУМВД активно занимается предотвращением и расследованием киберпреступлений, в том числе хакерских атак, мошенничества в сети Интернет и других компьютерных преступлений.

1.1.2 ЦИТС и ЗИ

Помимо основных задач, выполняемых ГУМВД по Амурской области, важным направлением работы является защита информации и обеспечение безопасности в сфере информационных технологий. В данной области значительный вклад вносит центр информационных технологий, связи и защиты информации (ЦИТМ и ЗИ), который является ответственным за создание и поддержание современной ИТ-инфраструктуры органов внутренних дел.

ЦИТС и ЗИ выполняет широкий спектр функций, включая:

– разработку и внедрение технических решений: отдел занимается разработкой и внедрением современных информационных технологий, систем связи и защиты данных. Здесь следят за инновациями в области информационной безопасности и обеспечивают использование передовых технологий и методов для защиты информации;

– управление информационной безопасностью: ЦИТС и ЗИ осуществляет контроль и мониторинг информационной безопасности органов внутренних дел. В рамках данной функции разрабатывается политика безопасности, проводятся аудиты и анализ уязвимостей, а также предпринимаются меры для предотвращения и реагирования на возможные угрозы и инциденты информационной безопасности;

– обучение и консультации: отдел проводит обучение и консультирует сотрудников органов внутренних дел в области информационной безопасности и правил использования информационных систем, а также содействует осведомленности сотрудников о рисках и мероприятиях по защите информации.

1.2 Структура управления и деятельности ЦИТС и ЗИ

1.2.1 Организационная структура ЦИТС и ЗИ

В центре информационных технологий, связи и защиты информации ГУМВД по Амурской области существует четкая организационная структура,

представленная на рисунке 1, которая способствует эффективному функционированию и координации задач в сфере защиты данных [16].

Рисунок 1 — Организационная структура ЦИТС и ЗИ

В данном подразделении выделяется несколько структурных единиц, в зависимости от численности персонала и объема задач, которые они выполняют.

Первой структурной единицей является отделение, которое формируется, когда в нем работает от 4 до 7 человек. Отделение представляет собой более крупную группу специалистов, которая выполняет различные функции и задачи в области технической защиты информации и компьютерной безопасности.

Второй структурной единицей является группа, которая формируется, когда в ней работает от 2 до 3 человек. Группа включает в себя более узкоспециализированных специалистов, которые занимаются определенными аспектами защиты информации или выполнением специфических задач.

Третьей структурной единицей является направление, которое формируется, когда в нем работает один человек. Направление может быть связано с руководством и координацией специализированных проектов, осуществлением аналитической работы или проведением научно-исследовательских и разработочных задач.

Приведенная структура позволяет эффективно организовывать работу,

учитывая численность и специализацию персонала. Она обеспечивает координацию и взаимодействие между специалистами, что способствует достижению высокого уровня безопасности информационных технологий и защите конфиденциальности данных.

1.2.2 Деятельность ЦИТС и ЗИ

В данной работе главным образом рассматривается политика информационной безопасности, формирующаяся кадровым составом предприятия. В связи с этим, было принято решение подробно рассмотреть деятельность центра информационных технологий, связи и защиты информации.

Одним из важных инструментов, использованных для анализа и визуализации этого процесса, является диаграмма деятельности, представленная на рисунке 2.

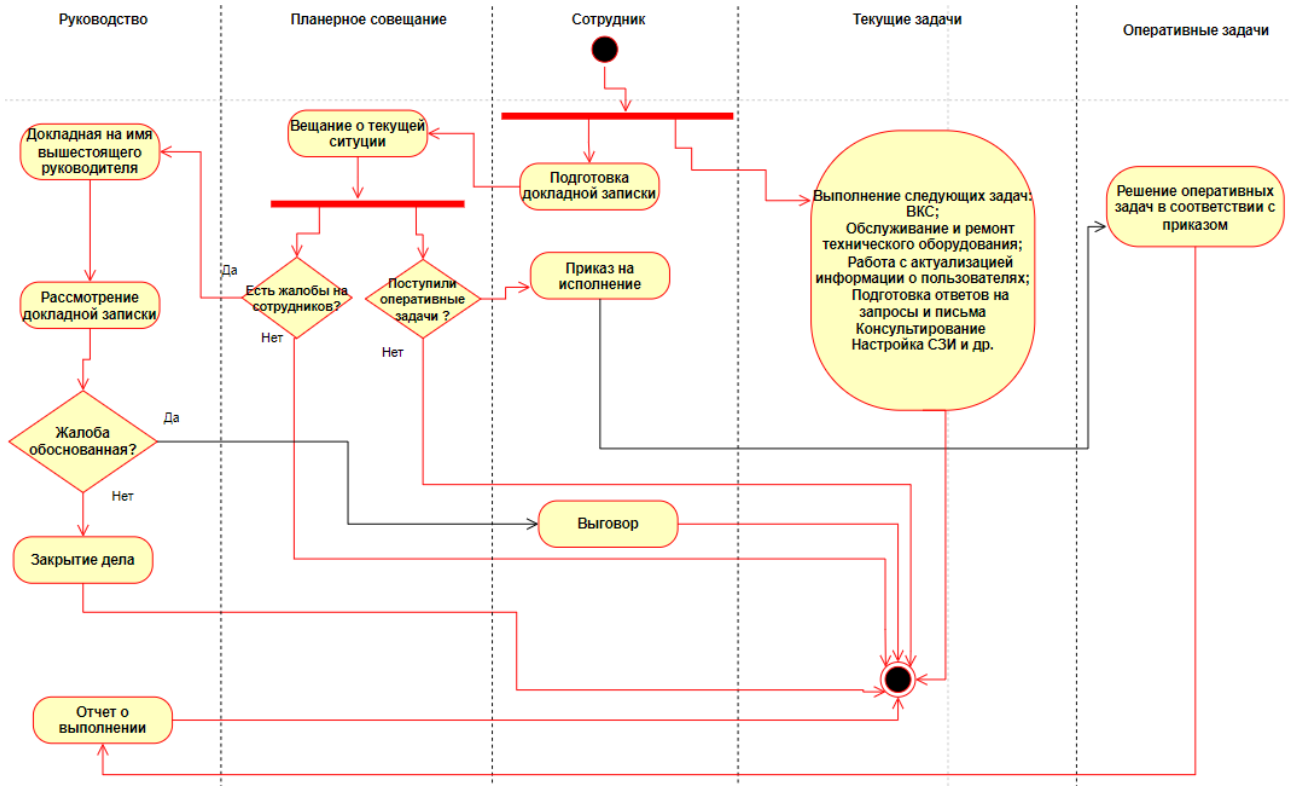

Рисунок 2 — Диаграмма деятельности ЦИТС и ЗИ

Данная диаграмма позволяет наглядно представить последовательность действий и процессов, которые выполняются в отделе ЦИТС и ЗИ для

обеспечения информационной безопасности.

1.3 Анализ существующих решений

IBM Kenexa Assess является одним из ведущих решений в области оценки уровня благонадежности соискателей. Этот продукт предоставляет широкий спектр инструментов для оценки профессиональных и личностных качеств кандидатов.

Данное решение:

– предлагает разнообразные профессиональные тесты и кейс-тестирование, адаптируемые под конкретные требования организации;

– включает психометрические тесты, основанные на научных исследованиях, для оценки личностных характеристик соискателей;

– обеспечивает гибкость в настройке и администрировании тестовых заданий, включая возможность добавления и удаления вопросов, изменения балльной системы и др;

– предоставляет подробные отчеты, включающие анализ результатов тестирования и рекомендации для рекрутеров.

IBM Kenexa Assess обладает широким функциональным набором для оценки кандидатов, включая профессиональные и личностные качества. Однако, для некоторых организаций может быть слишком сложным и дорогостоящим внедрение этой системы из-за высокой стоимости лицензирования и настройки.

Psychometrica – это программное решение, специализирующееся на оценке личностных качеств соискателей, которое предоставляет широкий набор психометрических тестов, разработанных на основе научных исследований.

Особенности Psychometrica включают возможность проведения разнообразных тестирований, которые измеряют такие характеристики, как лидерство, коммуникационные навыки, мотивация и другие аспекты личности. Программа обрабатывает полученные данные и предоставляет подробный анализ результатов, позволяя рекрутерам получить глубокое понимание

личностных качеств кандидатов и их сильных сторон. Psychometrica также обладает гибкостью и настраиваемостью, позволяя адаптировать тестовые задания под требования конкретной организации.

Однако следует отметить, что одним из недостатков Psychometrica является его ориентированность исключительно на оценку личностных качеств кандидатов. Программа не предоставляет инструментов для оценки профессиональных навыков и компетенций соискателей, что может быть недостатком для компаний, ценящих профессиональную подготовку кандидатов наравне с личностными чертами.

1.4 Обоснование необходимости создания программного продукта

Оценка уровня благонадежности соискателей на должность специалиста по защите информации является критическим фактором при подборе подобных специалистов. В свете этого, важно обеспечить высокий уровень доверия и надежности кандидатов, учитывая, что такие люди имеют доступ к конфиденциальным и критическим данным организации.

В то же время, с быстрым развитием информационных технологий и увеличением угроз кибербезопасности, специалисты по защите информации становятся неотъемлемой частью компаний.

В данном контексте создание программного продукта, специально адаптированного для оценки уровня благонадежности соискателей на должность специалиста по защите информации, является неотложной необходимостью. Разработанный механизм будет предоставлять надежный и эффективный инструмент для оценки потенциала и соответствия кандидатов требованиям в области кибербезопасности.

Программный продукт, созданный на основе профессионального стандарта № 06.033 «Специалист по защите информации в автоматизированных системах», обеспечит целевую оценку профессиональных компетенций и навыков, специфичных для данной должности. Он будет помогать организациям точнее определить потенциальные риски и принять взвешенное решение при выборе кандидата.

Кроме того, внедренный в программный продукт тест оценки личностных характеристик MMPI дополнительно обогатит процесс оценки соискателей. Благодаря MMPI будут получены данные о личностных особенностях соискателей, что поспособствует более глубокому пониманию их профиля.

Таким образом, организация сможет учесть не только профессиональные качества соискателей, но и их личностную пригодность, адаптируемость и потенциал для успешной работы в области защиты информации.

Следовательно, разработка программного обеспечения, учитывающего значимость оценки уровня благонадежности и уникальные требования к специалистам по защите информации в современном информационном контексте, обоснована и будет иметь существенное значение для эффективного подбора квалифицированных специалистов и обеспечения кибербезопасности организаций.

1.5 Выбор средств реализации программного продукта

При выборе средств разработки программного продукта имеется ряд альтернатив, каждая из которых предлагает свои особенности и возможности. В процессе анализа различных вариантов можно рассмотреть следующие средства разработки, представленные в таблице 1.

Таблица 1 — Средства разработки программного продукта

Категория	Средство разработки	Особенности
Языки программирования	C#	Объектно-ориентированный язык программирования. Широко используется для создания приложений на платформе .NET.
	Java	Высокоуровневый язык программирования, известный своей платформонезависимостью и использованием в различных областях разработки.
	Python	Интерпретируемый язык программирования с акцентом на читаемости кода и простоте использования.

Продолжение таблицы 1

Системы управления базами данных	MS SQL Server	Мощная система управления базами данных. Предоставляет надежное хранение, обработку данных и масштабируемость.
	MySQL	Одна из самых популярных систем управления базами данных с открытым исходным кодом. Обеспечивает гибкость и производительность.
	PostgreSQL	Мощная объектно-реляционная система управления базами данных с широким набором функций и поддержкой стандартов SQL.
Интегрированные среды разработки	Visual Studio	Интегрированная среда разработки, обеспечивающая полный набор инструментов для разработки приложений под платформу .NET.
	Eclipse	Популярная платформа разработки с открытым исходным кодом, которая поддерживает различные языки программирования и платформы.
	IntelliJ IDEA	Мощная интегрированная среда разработки для Java и других языков, предлагающая широкий спектр инструментов и функций для разработчиков.

После тщательного анализа всех вариантов можно сделать вывод, что наилучшим выбором для реализации программного продукта являются MS SQL Server, Visual Studio и язык разработки C#.

MS SQL Server обеспечивает надежное хранение и управление данными, а также предлагает широкий набор функций, таких как транзакции и процедуры хранения. Visual Studio, в свою очередь, предоставляет интегрированную среду

разработки с обширным набором инструментов для создания, отладки и тестирования приложений [22]. Язык разработки C# является мощным и гибким средством, который позволяет разрабатывать высокопроизводительные и масштабируемые приложения [15].

1.6 Определение требований к системе

Системные требования:

– система должна обеспечивать возможность одновременной работы нескольких пользователей, позволяя администраторам и кандидатам взаимодействовать с системой одновременно;

– система должна иметь механизмы защиты данных, включая аутентификацию пользователей, шифрование информации и обеспечение конфиденциальности персональных данных кандидатов;

– система должна быть способна масштабироваться для обработки большого количества кандидатов и данных, чтобы обеспечить эффективную работу даже при высокой загрузке;

– система должна быть стабильной и надежной, минимизируя возможность сбоев и потери данных;

– система должна интегрироваться с базой данных для хранения и управления информацией о кандидатах, тестах и результатов оценки.

Технические требования:

– система должна обеспечивать доступность как на персональных компьютерах, так и на ноутбуках;

– система должна иметь интуитивный и простой интерфейс пользователя, позволяющий кандидатам проходить тесты, а администраторам управлять системой без труда;

– система должна обеспечивать высокую производительность, обрабатывая запросы и отображая результаты тестов и оценок кандидатов быстро и эффективно;

– система должна быть совместимой с различными веб-браузерами и

операционными системами, чтобы обеспечить доступность для большинства пользователей.

Функциональные требования:

– система должна позволять проводить тестирование профессиональных и личностных качеств кандидатов, используя тесты и кейс-тестирование, а также отображать промежуточные результаты с количеством правильных ответов;

– система должна обеспечивать функциональность администрирования, позволяя администраторам добавлять, изменять и удалять тесты, кейс-тесты, вопросы, задания, а также настраивать баллы за ответы;

– система должна генерировать отчеты, содержащие все ответы кандидатов, с выделением правильных ответов зеленым цветом и неправильных ответов красным цветом.

Более детальные требования к описываемому продукту представлены в техническом задании на разработку проекта в приложении А.

2 ПРОЕКТИРОВАНИЕ ИНФОРМАЦИОННОЙ СИСТЕМЫ

2.1 Проектирование архитектуры ИС

2.1.1 Описание архитектуры ИС

Архитектура ИС оценки уровня благонадежности соискателя на должность специалиста по защите информации будет состоять из четырех основных компонентов: клиентского приложения, серверной части, базы данных и внешнего сайт, а также API для обмена данными между представленными элементами [1].

– клиентское приложение содержит пользовательский интерфейс и осуществляет взаимодействие с серверной частью системы;

– серверная часть системы обрабатывает запросы клиентского приложения и выполняет следующие функции:

– хранение и управление базой данных пользователей и администраторов, вопросами тестов и кейс-тестов, требованиями для генерации тестов и кейс-тестов, перечнем для формирования рекомендаций;

– генерация тестов и кейс-тестов на основе данных, введенных пользователем при заполнении анкеты, и требований, заданных администратором;

– формирование перечня рекомендаций на основе допущенных ошибок;

– расчет промежуточного и общего уровня благонадежности кандидата на основе результатов ответов на тесты и кейс-тесты;

– обработка запросов администраторов на изменение вопросов тестов, кейс-тестов и списка рекомендаций, создание новых тестов, кейс-тестов и списков рекомендаций, создание и управление учетными записями администраторов, формирование отчетов о кандидатах;

– предоставление интерфейса для взаимодействия приложения с внешним сайтом;

– обработка результатов теста, представленных внешним сайтом.

– база данных, которая хранит информацию о пользователях, администраторах, рекомендациях, вопросах тестов и кейс-тестов, результаты ответов на тесты и кейс-тесты, а также настройки требований для генерации тестов и кейс-тестов;

– сторонний сайт для прохождения теста: система взаимодействует с внешним сайтом, где расположен личностный тест, который должен пройти соискатель;

– API для взаимодействия клиентского приложения, серверной части системы и внешнего сайта, который содержит методы для отправки запросов на сервер и получения ответов.

2.1.2 Схема взаимодействия компонентов архитектуры ИС

Для того, чтобы создать схему взаимодействия компонентов информационной системы, требуется определить, каким образом данные компоненты взаимодействуют друг с другом.

Клиентское приложение отправляет запрос на серверную часть через API.

Серверная часть получает запрос и проверяет, аутентифицирован ли пользователь. Если нет, серверная часть отправляет запрос на авторизацию пользователя.

Серверная часть проверяет права доступа пользователя на выполнение данного запроса в соответствии с бизнес-логикой ИС.

Если запрос требует доступа к базе данных, серверная часть отправляет запрос на базу данных и получает ответ.

Также серверная часть отправляет запрос на сторонний сайт, получает ответ и анализирует полученные данные в соответствии с бизнес-логикой ИС.

Серверная часть формирует ответ на запрос и отправляет результат обратно клиентскому приложению через API.

Клиентское приложение получает и обрабатывает ответ, отображая результаты пользователю.

Изображение 3 представляет общую архитектуру разрабатываемой системы.

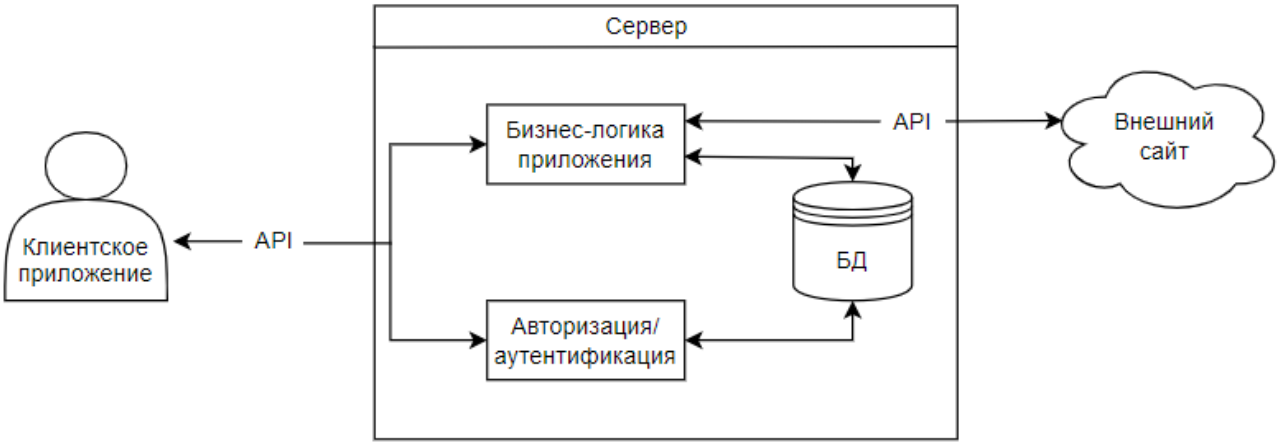

Рисунок 3 — Схема архитектуры ИС

По данной архитектуре можно выделить несколько преимуществ:

– разделение обязанностей между клиентским приложением и серверной частью позволяет достичь более гибкой и масштабируемой системы;

– использование стороннего сайта для прохождения личностного теста снижает трудозатраты на разработку и обслуживание системы, поскольку нет необходимости создавать и поддерживать свой собственный функционал для прохождения данного теста;

– проверка прав доступа пользователя на выполнение запроса позволяет обеспечить безопасность системы и защиту пользовательских данных;

– использование API для обмена данными между клиентским приложением и серверной частью позволяет создать более гибкую и расширяемую систему, которая может работать с различными типами данных и интегрироваться с другими системами.

2.2 Проектирование БД ИС

2.2.1 Инфологическое проектирование БД

Для создания качественной базы данных необходимо провести инфологическое проектирование, которое позволяет определить основные объекты предметной области и связи между ними. В рамках данной работы были выделены ключевые сущности, которые будут отражены в БД:

Кандидат – это сущность, которая представляет собой соискателя, проходящего отбор на вакансию.

Администратор – это сущность, которая имеет права доступа к системе и может управлять объектами данной системы.

Тест – это сущность, которая представляет собой набор вопросов, на которые должен ответить кандидат.

Кейс-тест – это сущность, которая представляет собой специализированный тест для оценки навыков соискателя в определенной области.

Тестовые вопросы – это сущность, которая содержит вопросы, используемые в тестах.

Кейс-задания – это сущность, которая содержит задания, используемые в кейс-тестах.

Темы вопросов и заданий – это сущность, которая содержит темы, к которым относятся тестовые вопросы и кейс-задания.

Требования – это сущность, которая содержит информацию о требованиях к генерации тестов для соискателей.

Анкетирование – это процесс, который позволяет получить информацию от кандидата о его опыте, образовании и других важных деталях.

Результаты (ответы) тестирования – это сущность, которая содержит в себе ответы кандидата на тестовые вопросы.

Результаты (ответы) кейс-тестирования – это сущность, которая содержит в себе ответы кандидата на кейс-тестовые задания.

При инфологическом проектировании БД, помимо выделения сущностей, важным этапом является определение атрибутов данных сущностей и описание связей между объектами. Однако, необязательно включать описание каждой связи в текст проекта. Вместо этого, на общей инфологической модели, представленной на рисунке 4 все связи отражены сразу, позволяя получить полное представление о структуре базы данных.

Атрибуты же каждой сущности будут представлены в логической модели данных, что обеспечит полноту и точность информации.

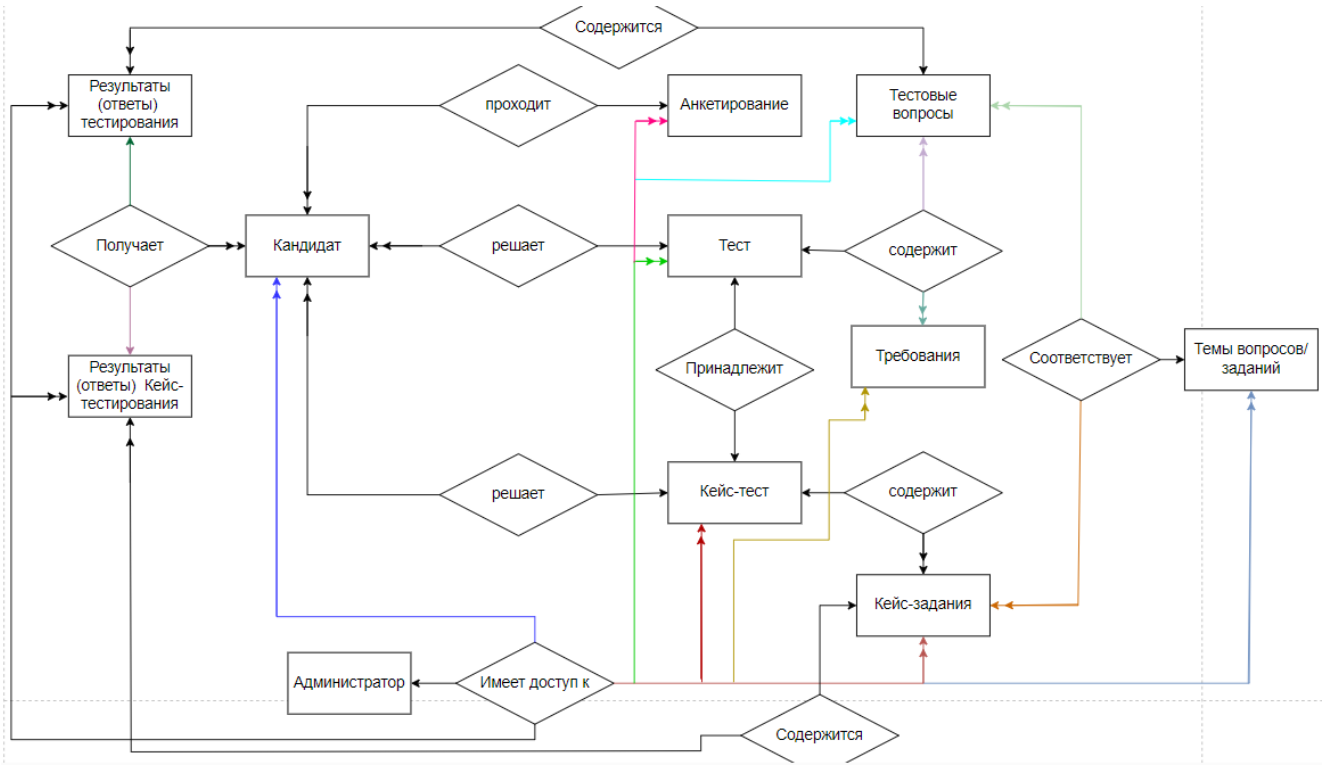

Рисунок 4 — Инфологическая модель БД

Инфологическая модель является основой для дальнейшего физического проектирования БД.

2.2.2 Логическое проектирование БД

На основе инфологической модели, разработанной на предыдущем этапе, проводится логическое проектирование базы данных, в результате которого определяется структура БД и ее основные характеристики.

Логическая схема базы данных представляет собой конкретное решение по реализации инфологической модели в базе данных [6]. Процесс преобразования включает в себя перевод сущностей и связей диаграммы в соответствующие таблицы базы данных, атрибутов – в поля таблиц, а также определение ограничений на связи между таблицами, на валидность данных и другие важные аспекты.

На рисунке 5 представлена логическая модель базы данных, где каждая таблица представляет отдельную сущность с ее атрибутами. В таблице «Администратор» отсутствуют внешние ключи, связывающие ее с другими таблицами. Это объясняется тем, что в приложении реализован механизм

авторизации, который позволяет администратору получать доступ ко всем объектам в приложении на уровне логики. Таким образом, на логической модели базы данных не было установлено связей с таблицей «Администратор», но в инфологической модели была добавлена связь «Имеет доступ к» для наглядности и лучшего понимания взаимосвязей между сущностями.

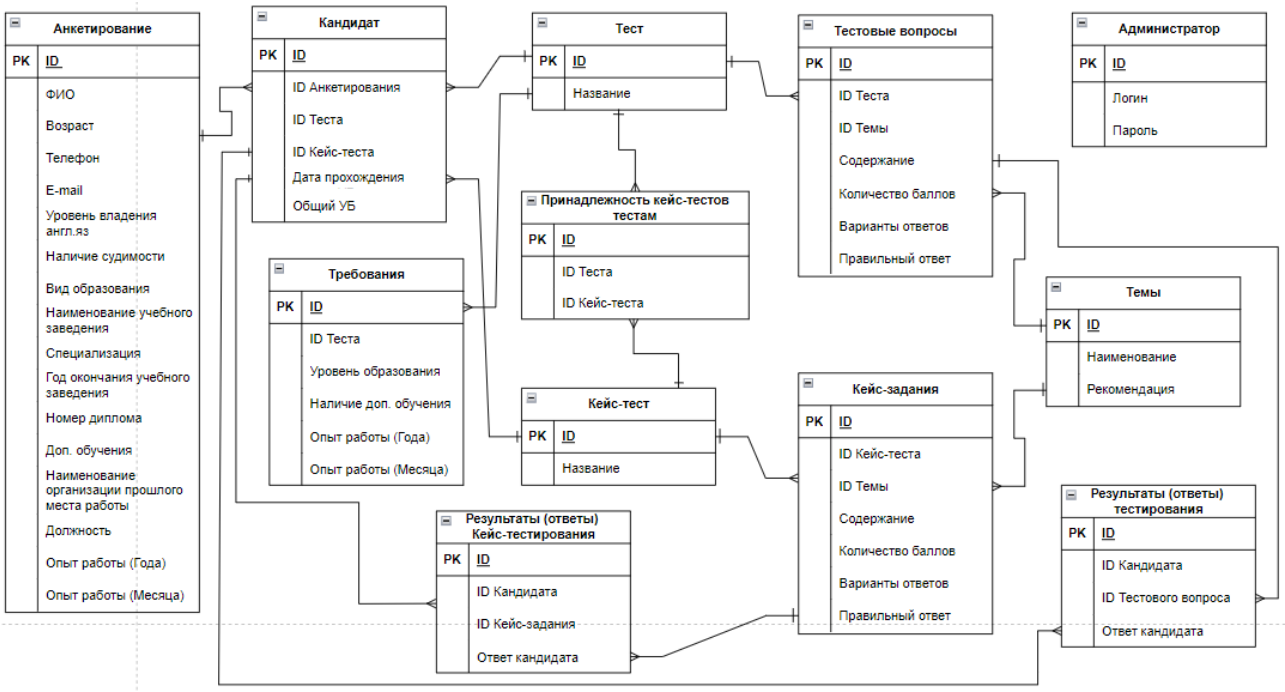

Рисунок 5 — Логическая модель БД

Теперь, имея логическую модель, можно приступать к физическому проектированию и созданию реальной базы данных, которая будет поддерживать работу создаваемого приложения.

2.2.3 Физическое проектирование БД

На основе логической модели базы данных, созданной в предыдущем разделе, необходимо разработать физическую модель, учитывая конкретную СУБД – MS SQL. Физическая модель определяет типы данных, ограничения целостности, индексы и другие аспекты, необходимые для эффективной работы с базой данных в конкретной среде.

В физической модели БД, представленной на рисунке 6, каждой сущности и ее атрибутам соответствует определенный тип данных, а также указаны внешние ключи, связывающие сущности между собой.

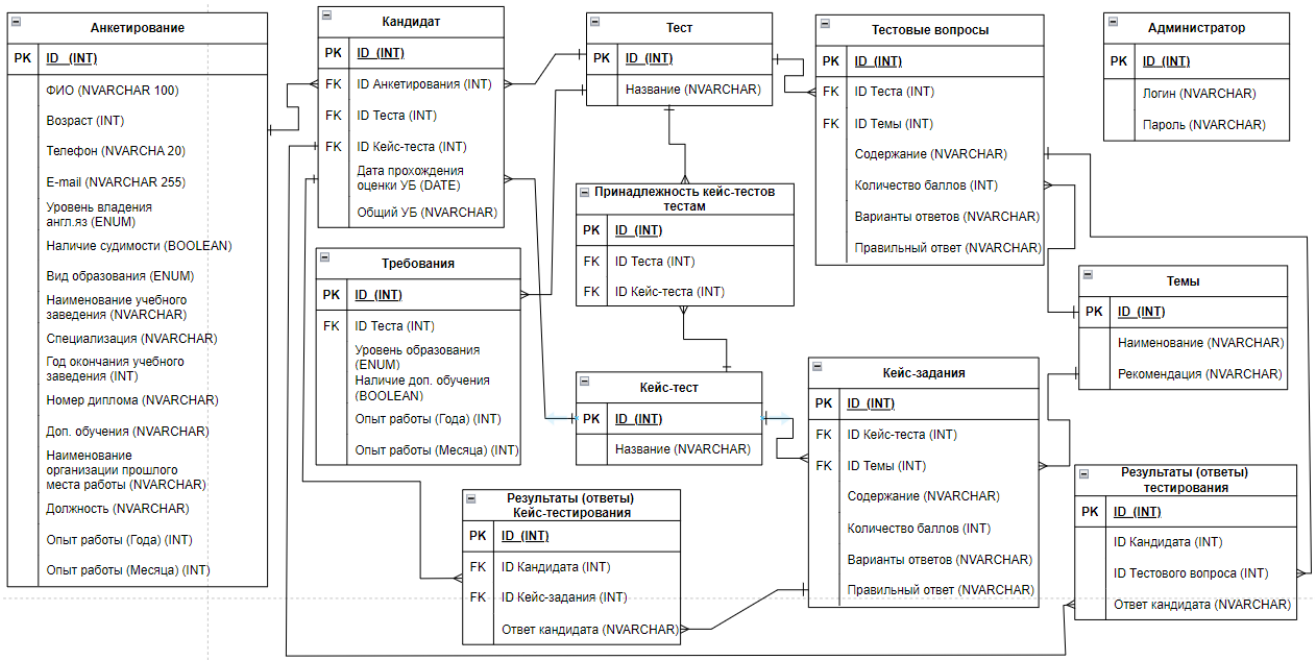

Рисунок 6 — Физическая модель БД

В процессе создания физической модели были учтены все требования к БД, определенные в логической модели, а также все особенности выбранной СУБД. Полученная физическая модель базы данных позволяет эффективно хранить и обрабатывать данные в рамках разрабатываемого приложения.

2.3 Проектирование пользовательского интерфейса

2.3.1 Описание требований к пользовательскому интерфейсу

В данном разделе в таблице 2 приводится описание элементов пользовательского интерфейса ИС, необходимых для выполнения функций и обеспечения удобства использования.

Таблица 2 — Требования к пользовательскому интерфейсу

Требование	Описание
Расположение элементов	Элементы управления должны быть расположены интуитивно понятно и удобно для пользователя. Важно обеспечить логическую последовательность и иерархию элементов, чтобы обеспечить простоту и быстроту доступа к нужной информации.
Размер элементов	Размер элементов должен быть достаточным, чтобы пользователь мог легко и точно управлять ими, включая кнопки, поля ввода, выпадающие списки и т.д.
Дизайн	Дизайн пользовательского интерфейса должен быть современным и эстетичным, соответствующим общей

Продолжение таблицы 2

	стилистике приложения. Важно использовать легко читаемый шрифт, подходящие цвета и графику (применение светлых цветов фона и темных цветов текста), а также оптимизировать дизайн для разных устройств и разрешений экранов.
Иконки	Иконки элементов управления должны быть понятными и наглядными, чтобы пользователь мог быстро идентифицировать нужный элемент и понять, что он делает.
Подсказки и инструкции	Важно предоставлять пользователю понятные и лаконичные подсказки, когда это необходимо, а также обеспечивать доступ к инструкциям для более подробной информации о последующих действиях.
Адаптивность	Интерфейс должен быть адаптивным, чтобы адекватно отображаться на различных устройствах и в разных ориентациях экрана. Это может включать изменение размеров и расположения элементов, а также адаптацию дизайна и графики.

При проектировании интерфейса необходимо учитывать все перечисленные выше требования, чтобы обеспечить удобство и эффективность работы пользователей с системой.

2.3.2 Разработка макетов пользовательского интерфейса

В рамках проектирования информационной системы были разработаны макеты пользовательского интерфейса, которые представляют собой набор графических элементов, упорядоченных в соответствии с логикой работы системы. Кроме того, были созданы макеты анкет, тестов и форм редактирования данных, которые предназначены для взаимодействия пользователей с системой.

Для наглядного представления разработанные макеты, продемонстрированы на рисунках 7–16.

Создание макетов форм пользовательского интерфейса способствует более эффективной разработке и более удовлетворительному конечному результату, соответствующему требованиям и ожиданиям пользователей. Они также позволяют оптимизировать пользовательский опыт и удобство

использования системы, предварительно выявляя возможные проблемы и улучшения интерфейса.

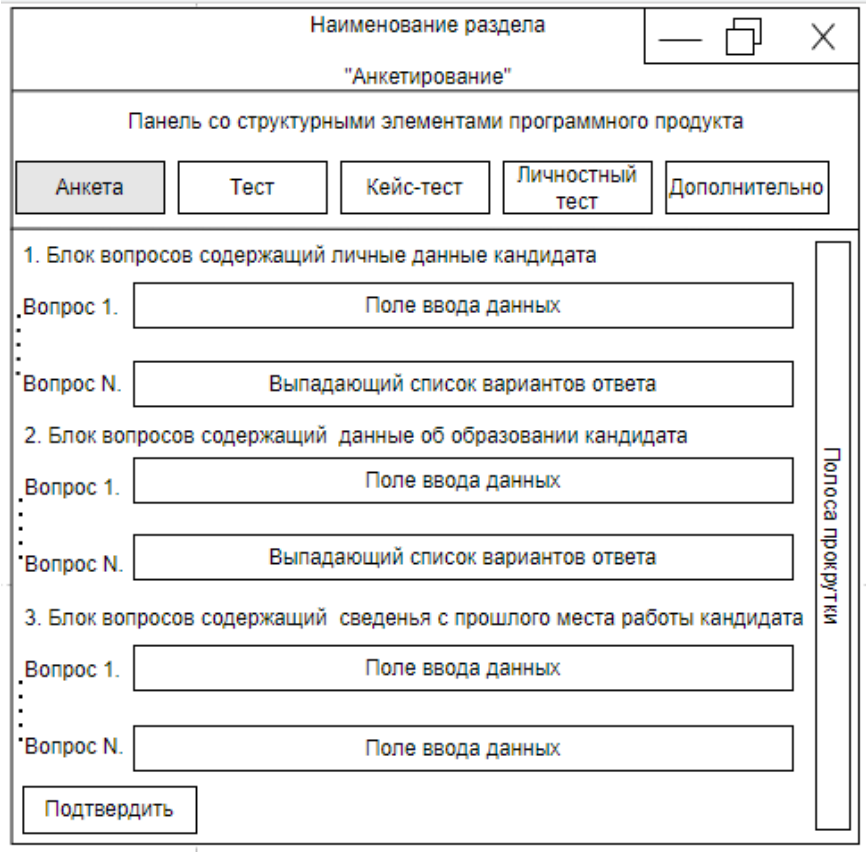

Рисунок 7 — Макет формы «Анкета»

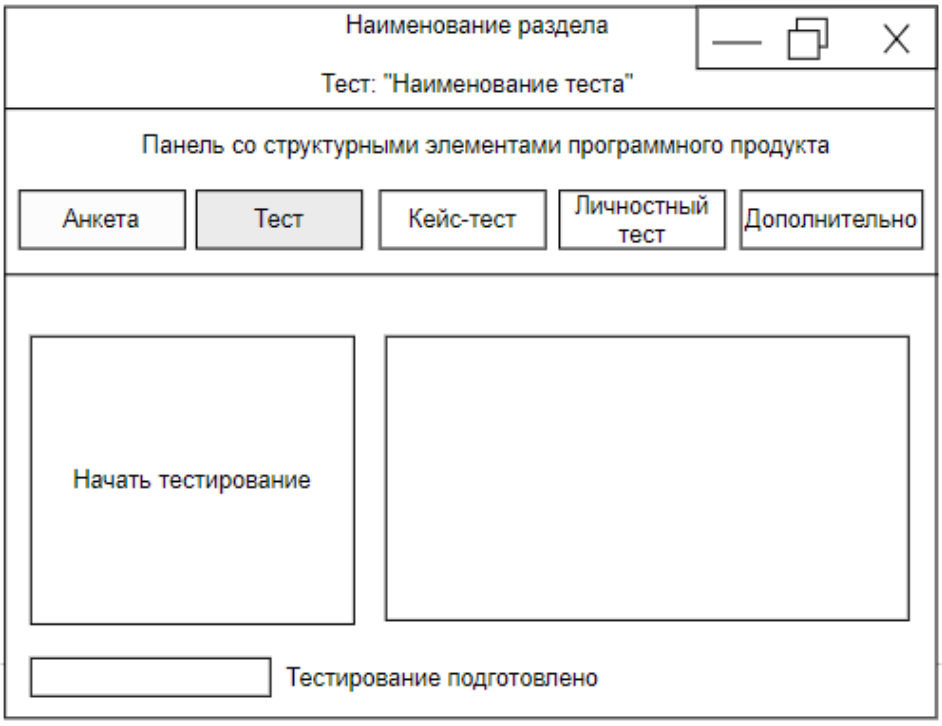

Рисунок 8 — Макет формы перехода между формами «Анкета» и «Тест»

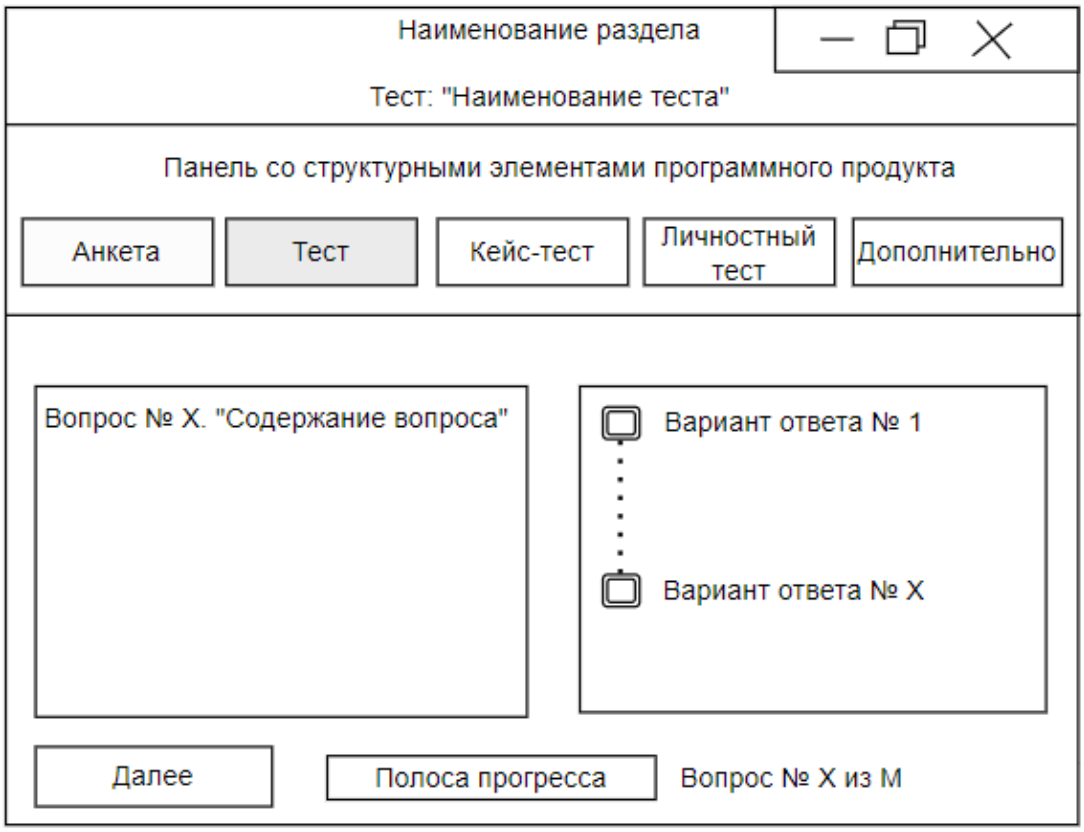

Рисунок 9 — Макет формы «Тест»

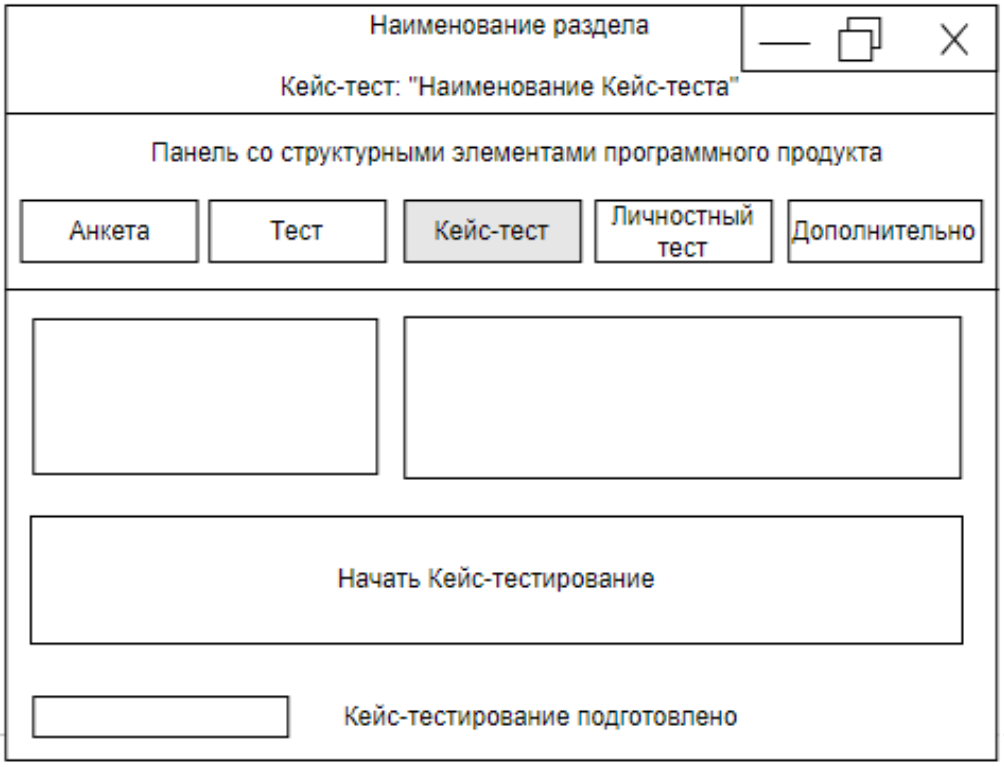

Рисунок 10 — Макет переходной формы между формами «Тест» и «Кейс-тест»

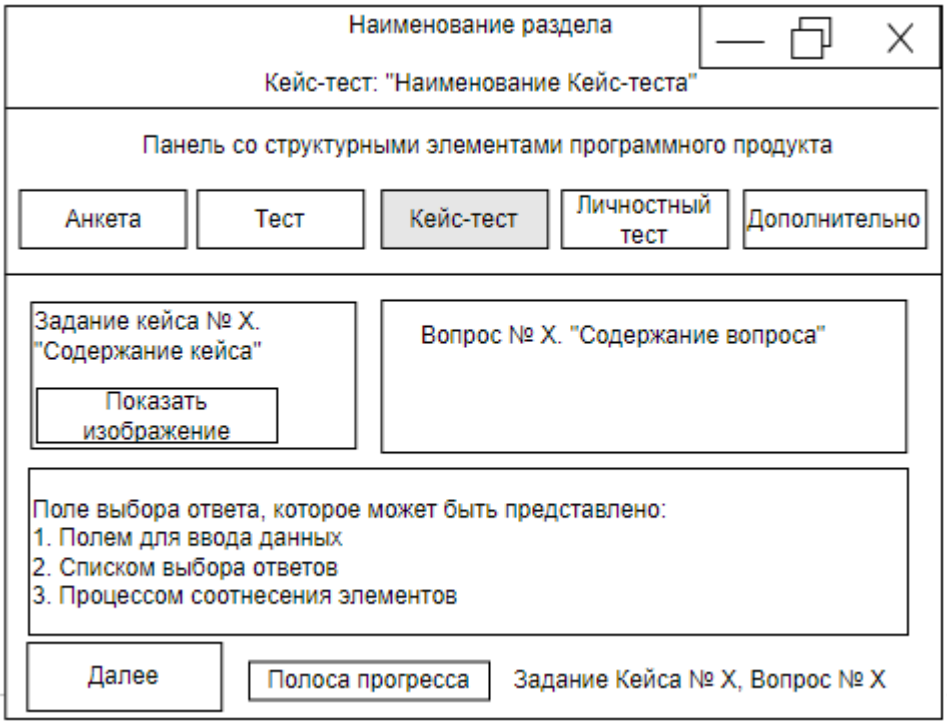

Рисунок 11 — Макет формы «Кейс-тест»

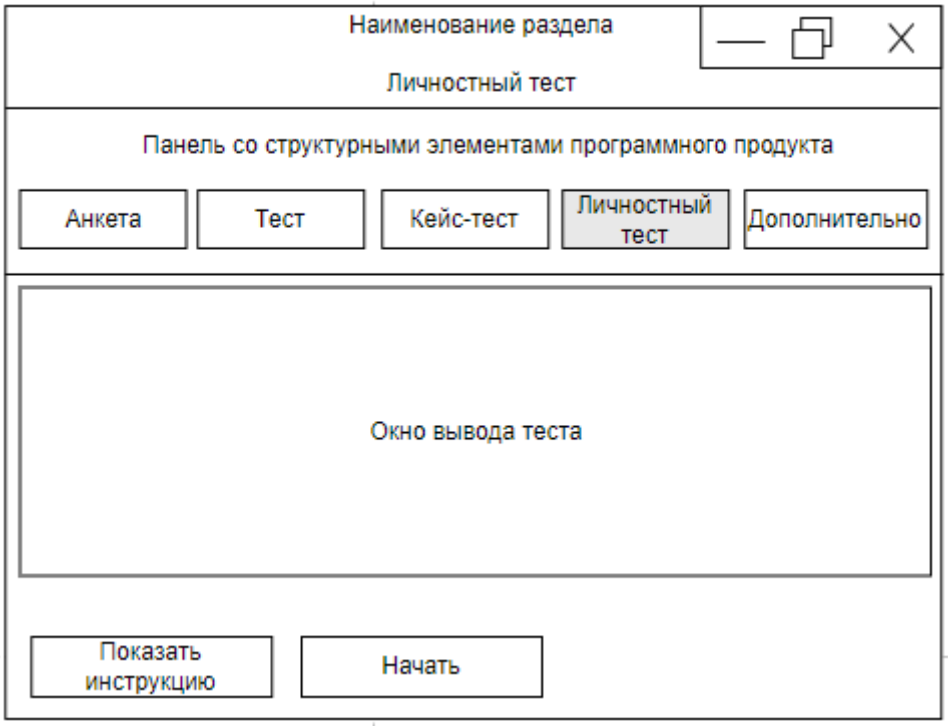

Рисунок 12 — Макет формы «Личностный тест»

Для вкладки «Дополнительно» отдельный макет не разрабатывался, поскольку данный раздел содержит всего два элемента – кнопку для авторизации на сервере и поле для указания пути сохранения отчета. Данные

элементы интегрированы в общий дизайн пользовательского интерфейса, разработанный для системы.

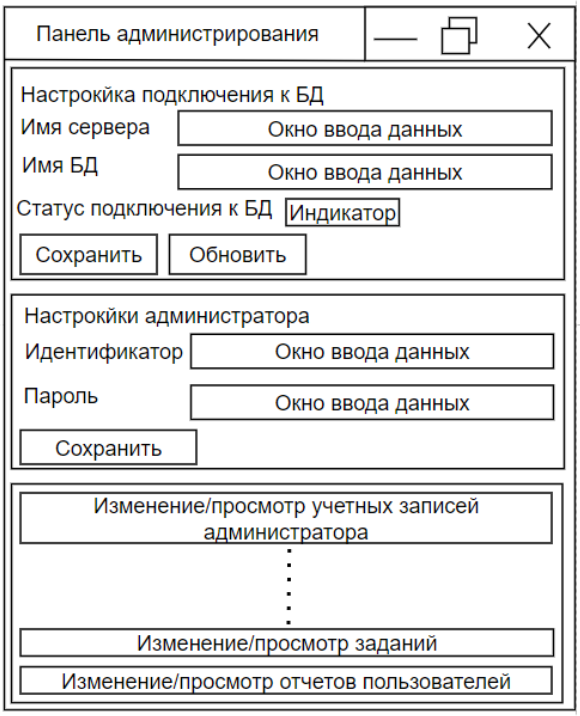

Рисунок 13 — Макет панели администрирования

Для действий администратора, таких как изменение и просмотр элементов системы, был разработан единый макет форм интерфейса. Все элементы взаимодействия соответствуют общему дизайну и принципу работы.

Рисунок 14 — Макет формы просмотра и изменения элементов системы

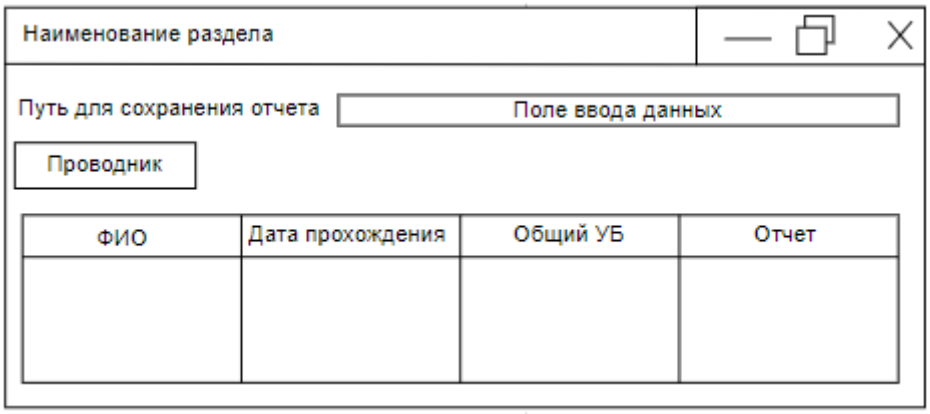

Рисунок 15 — Макет формы просмотра отчетов пользователей

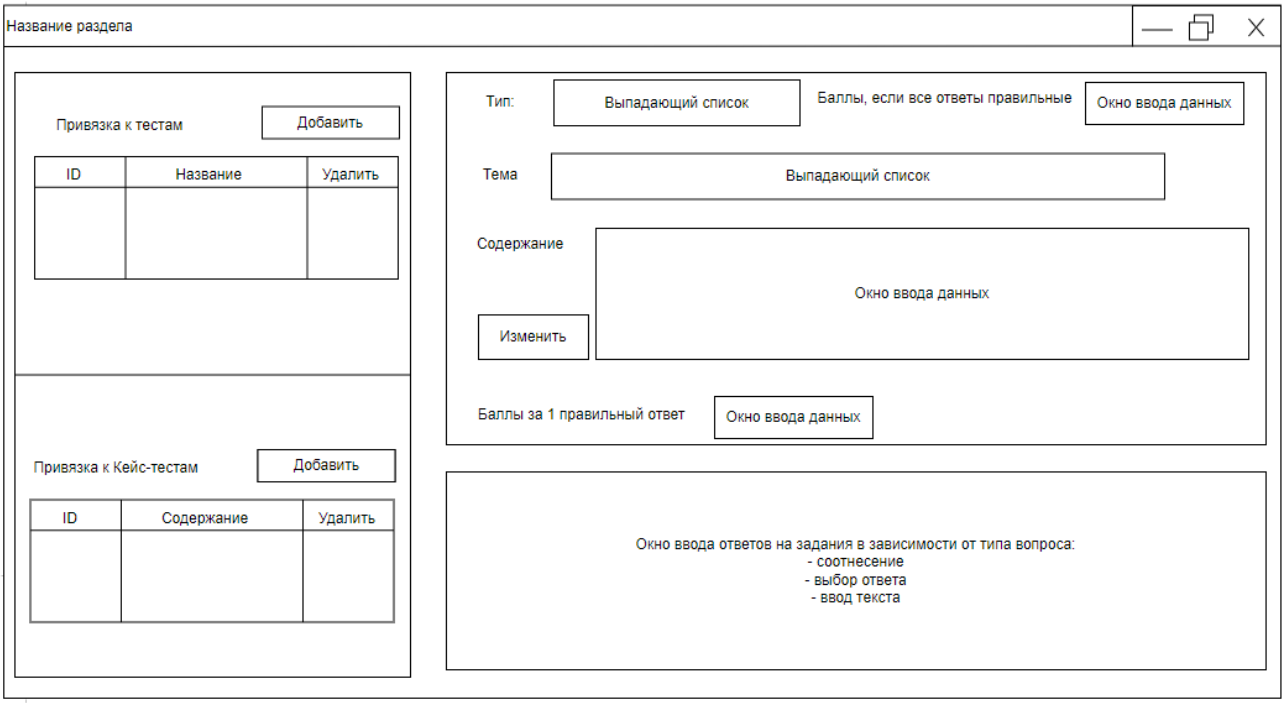

Рисунок 16 — Макет формы создания тестовых вопросов и кейс-заданий

Разработанные макеты учитывают требования по удобству использования и функциональности, а также соответствуют всем ранее определенным условиям к пользовательскому интерфейсу и элементам.

Каждый макет имеет свою уникальную структуру и набор элементов, которые обеспечивают пользователей всей необходимой информацией и удобством в использовании системы. Макеты анкет, тестов и форм редактирования данных предоставляют возможность пользователям быстро и эффективно работать с данными, вводить, редактировать и сохранять информацию.

В целом, разработанные макеты являются интуитивно понятными и легкими в использовании, что позволяет пользователям быстро адаптироваться к системе и использовать данную разработку в повседневной работе.

2.4 Проектирование методики оценки уровня благонадежности

2.4.1 Теоретический фундамент исследований ведущего источника

Теоретический фундамент исследований ведущего источника играет определяющую роль в разработке собственной методики. Обращение к трудам Александра Александровича Шелупанова – российского ученого, доктора технических наук, профессора и основателя научной школы «Фундаментальные и прикладные основы в области проектирования и разработки комплексных систем обеспечения информационной безопасности, защиты информации» является логичным выбором.

Исследования Шелупанова получили широкое признание в научном сообществе и считаются авторитетными источниками в области проектирования комплексных систем обеспечения информационной безопасности. Его работы предоставляют ценные теоретические основы и практические рекомендации, которые необходимы для разработки эффективной методики.

Использование теоретического фундамента, разработанного Александром Александровичем, позволяет применить проверенные и инновационные подходы в работе. Это обеспечивает надежность, качество и признание методики в научной среде, а также подчеркивает стремление к использованию передовых научных разработок.

В результате, основываясь на теоретическом фундаменте исследований ведущего источника – А. А. Шелупанова, создана собственная методика, которая сочетает академические принципы с практической применимостью в области проектирования комплексных систем обеспечения информационной безопасности.

2.4.2 Описание методики оценки уровня благонадежности соискателя

Методика расчета уровня благонадежности основана на следующих составляющих:

Первая составляющая – анкетирование. Этот элемент является отправной точкой в процессе оценки уровня благонадежности и содержит три блока вопросов: личные данные, образование и сведения с прошлого места работы. На основе предоставленных данных система генерирует тест для оценки профессиональных качеств кандидата.

Вторая составляющая методики – тестирование, основанная на профессиональном стандарте № 06.033 «Специалист по защите информации в автоматизированных системах». Для разработки тестов были выделены три обобщенных трудовых функции, каждая из которых включает перечень вопросов, связанных с соответствующей областью. Тестирование предлагает вопросы разного уровня сложности, отражающие требуемый уровень образования, навыков и опыт работы кандидата.

Третья составляющая – кейс-тестирование. Этот элемент также направлен на оценку профессиональных качеств, однако кандидат может приступить к решению кейсов только после правильного ответа на 60 % и более тестовых вопросов. Всего имеется три кейс-тестирования, принадлежащих каждому из тестов.

Четвертая составляющая – личностный тест. Этот элемент направлен на оценку личностных качеств кандидата, таких как:

– тенденция испытуемого представить себя в возможно более выгодном свете, продемонстрировать очень строгое соблюдение социальных норм;

– отсутствие откровенности, стремление скрыть дефекты своего характера и наличие каких-либо проблем и конфликтов;

– тенденция переложить ответственность за существующие проблемы на окружающих;

– преобладание пассивности личностной позиции;

– неустойчивость эмоций и конфликтное сочетание разнонаправленных тенденций;

– активная личностная позиция, высокая поисковая активность;

– устойчивость интересов, упорство в отстаивании собственного мнения, стеничность установок;

– высокая мотивация достижения;

– неуверенность в себе и в стабильности ситуации, высокая чувствительность и подвластность средовым воздействиям;

– аналитический склад мышления;

– обращенность интересов в мир внутренних переживаний и др.

К данному тесту допускаются кандидаты, успешно решившие 60 % и более кейсовых заданий.

После завершения всех этапов формируется общая оценка уровня благонадежности по 100% шкале согласно следующей формуле (1):

$$0{,}2 * (О) + 0{,}3 * (СР) + 0{,}5 * ((0{,}5 * (ПК)) + (0{,}5 * (ЛД))), \quad (1)$$

где – О коэффициент уровня образования;

СР – коэффициент стажа работы;

ПК – коэффициент профессиональных компетенций;

ЛД – коэффициент личностных данных.

Коэффициенты уровня образования и стажа работы представлены в таблицах 3 – 4 соответственно [20].

Коэффициент профессиональных компетенций – это среднее арифметическое по результатам правильно данных ответов на тестовые и кейс-тесовые задания.

Коэффициент личностных данных – это среднее арифметическое по результатам ответов, которые входят в норму того или иного вида психометрического оценивания.

Таблица 3 — Коэффициенты уровня образования

Уровень образования	Значение коэффициента
Основное общее образование	0,1

Продолжение таблицы 3

Среднее общее образование	0,2
Основное общее образование + Дополнительное обучение, сертификаты	0,3
Среднее общее образование + Дополнительное обучение, сертификаты	0,4
Среднее профессиональное образование	0,5
Высшее образование – бакалавриат	0,6
Высшее образование – специалитет, магистратура	0,7
Среднее профессиональное образование + Дополнительное обучение, сертификаты	0,8
Высшее образование – бакалавриат + Дополнительное обучение, сертификаты	0,9
Высшее образование – специалитет, магистратура + Дополнительное обучение, сертификаты	1

Таблица 4 — Коэффициенты стажа работы

Стаж работы	Значение коэффициента
Без опыта	0
До 1 года	0,2
От 1 до 3 лет	0,4
От 3 до 6 лет	0,6
От 6 до 10 лет	0,8
Свыше 10 лет	1

Таким образом, при оценке уровня благонадежности кандидата на трудоустройство используется процентное значение, полученное в результате соответствующей проверки. Данное значение отражает степень надежности и навыков соискателя, а также его потенциал для будущего развития.

В соответствии с заданными условиями, полученные процентные значения классифицируются в три категории:

– низкий уровень благонадежности 40 % или менее;

– средний уровень благонадежности от 41 % до 65 %;

– высокий уровень благонадежности от 66 % до 100 %.

Каждая из этих категорий имеет свои последствия для соискателя: отказ в трудоустройстве для кандидатов с низким уровнем благонадежности, предложение работы с перспективой обучения для кандидатов со средним уровнем благонадежности и приоритетное рассмотрение для кандидатов с высоким уровнем благонадежности.

Разработанная система оценки поможет работодателям принять информированные решения при отборе кандидатов и определении их дальнейшей карьерной траектории.

3 РЕАЛИЗАЦИЯ ПРОГРАММНОГО ПРОДУКТА

3.1 Модули и компоненты ИС через структуру реализуемого проекта

Модуль аутентификации и авторизации представляется следующими компонентами:

Алгоритм аутентификации пользователей:

– при получении запроса на аутентификацию от пользователя, модуль аутентификации получает логин и пароль;

– модуль аутентификации извлекает зашифрованный пароль из базы данных, сверяет введенный пароль с сохраненным зашифрованным паролем;

– если пароли совпадают, аутентификация проходит успешно, и пользователь считается подлинным.

Реализация выше описанного алгоритма происходит через окно формы представленной на рисунке 17 и логику приложения, исполняемую через класс «Encryption.cs» в проекте программы, представленном на рисунке 18.

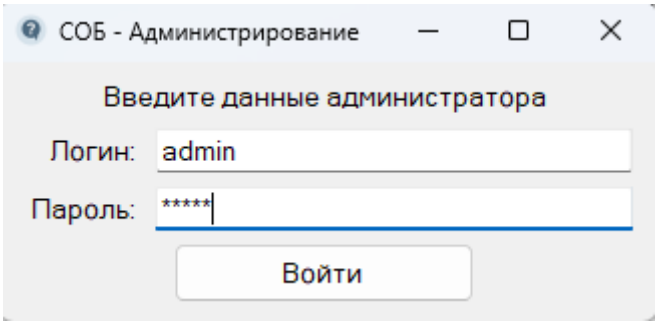

Рисунок 17 – Окно формы аутентификации и авторизации

Реализация функций авторизации и управления правами доступа:

– после успешной аутентификации пользователя, модуль авторизации присваивает пользователю соответствующие права доступа, определяющие его роль в системе (администратор);

– модуль авторизации проверяет права доступа пользователя перед выполнением определенных операций. Пользователь в роли администратора может добавлять, изменять и удалять тесты, кейс-тесты, вопросы и задания, а также другие компоненты ИС.

Данные действия также реализуются логикой приложения, исполняемой через класс «DataManag.cs» в проекте программы, представленном на рисунке 18 и форму администрирования, приведенную на изображении 19.

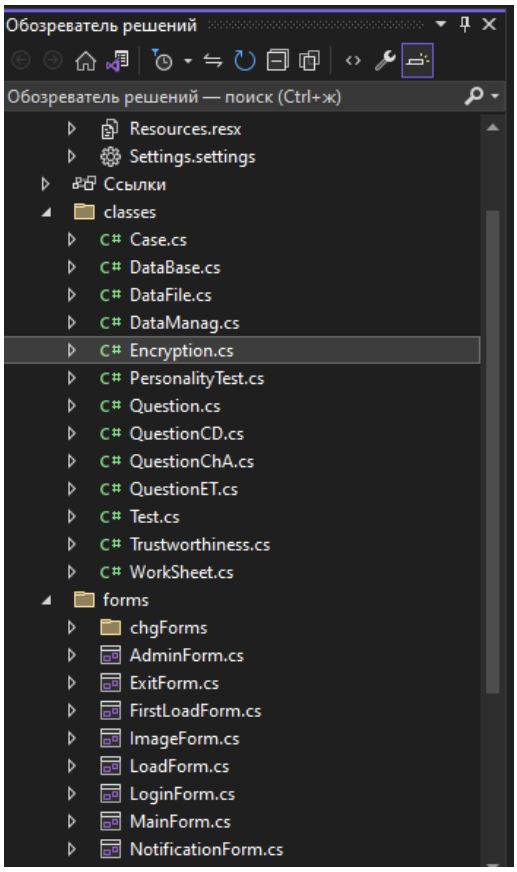

Рисунок 18 — Проект разработки программного продукта

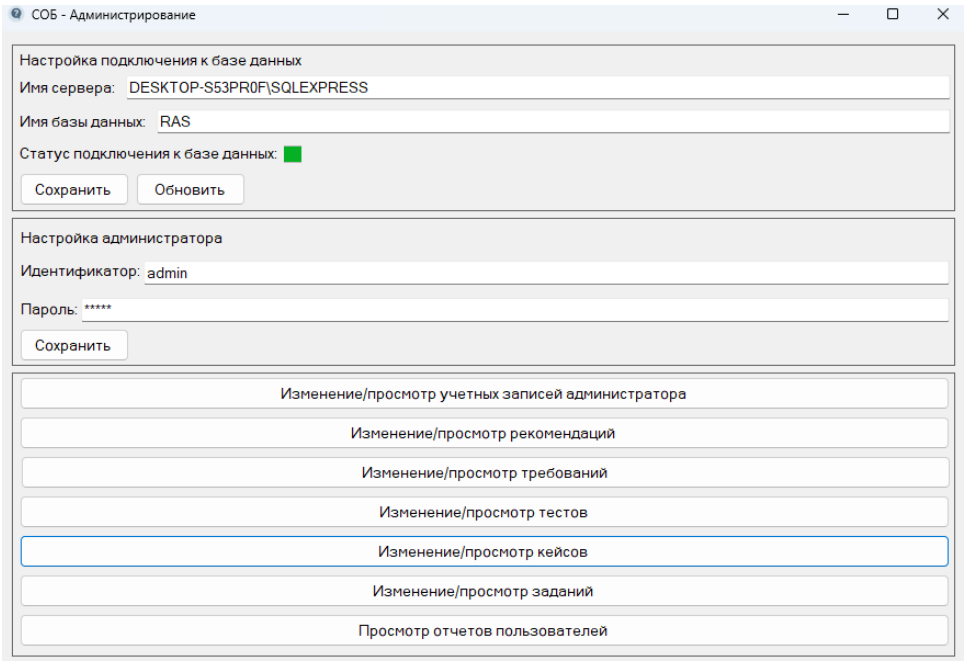

Рисунок 19 — Форма администрирования

Обеспечение безопасности данных и конфиденциальности персональной информации:

– защита паролей администраторов в базе данных с помощью шифрования;

– использование безопасного соединения с базой данных для передачи данных, через протокол HTTPS, чтобы предотвратить несанкционированный доступ к информации;

– защита конфиденциальной информации, такой как персональные данные кандидатов, с использованием соответствующих механизмов шифрования.

Выше описанные компоненты реализуются уже через знакомый класс проекта – «Encryption.cs».

Модуль управления данными отвечает за управление системой и выполнением административных функций и представляется через:

Управление пользователями – данный элемент позволяет администраторам создавать новых пользователей, редактировать существующих и удалять их из системы.

Управление тестами и кейс-тестами:

– предоставляет возможность добавления новых тестов и кейс-тестов в систему;

– администраторы могут редактировать и удалять существующие тесты, кейс-тесты, вопросы и задания;

– для каждого теста или кейс-теста можно настраивать баллы за ответы и определять правильные ответы.

Генерация отчетов:

– модуль позволяет генерировать различные отчеты, связанные с процессом тестирования и оценки кандидатов;

– отчеты могут содержать информацию о прохождении тестов, результаты оценки кандидатов и другие сводные данные.

Модуль управления данными предоставляет удобный интерфейс для администраторов системы, позволяющий эффективно управлять элементами информационного продукта, пользователями и базой данных. Разработанный модуль играет важную роль в обеспечении функциональности и гибкости системы, а также обеспечивает удобство в использовании.

Реализация данного модуля осуществлена через классы «DataManag.cs» и «WorkSheet.cs» изображенные на рисунке 18 и формы, представленные на картинках 20 – 24.

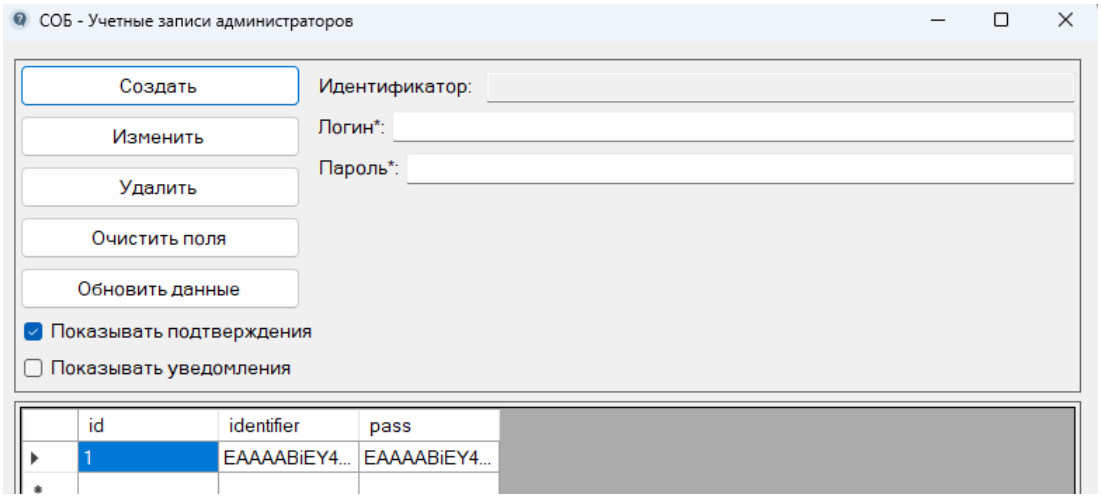

Рисунок 20 — Форма управления пользователями

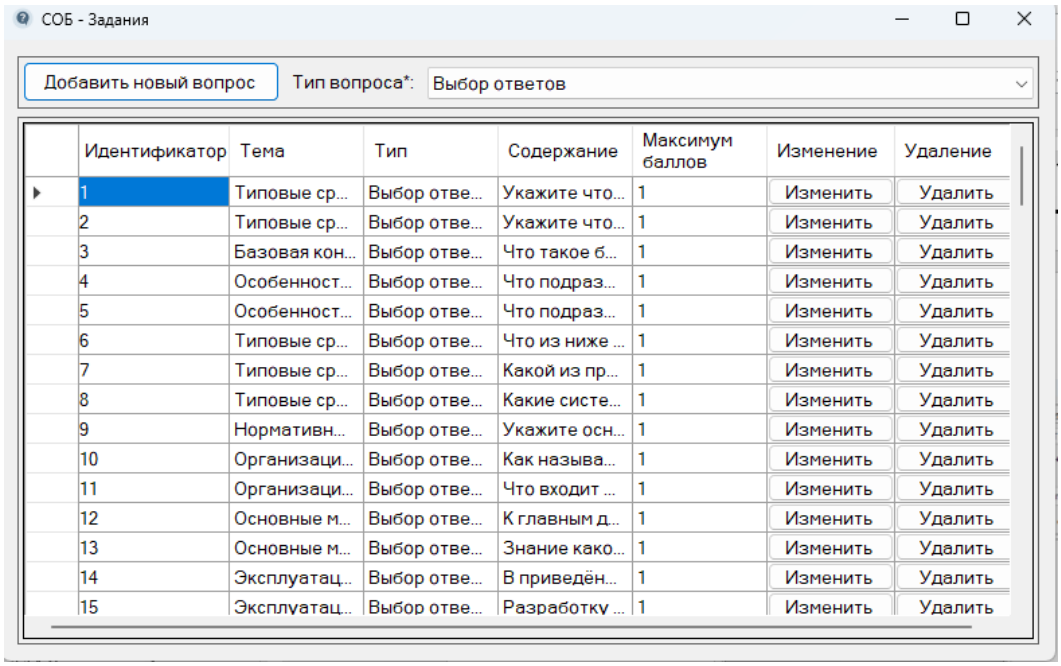

Рисунок 21 — Форма управления вопросами и заданиями

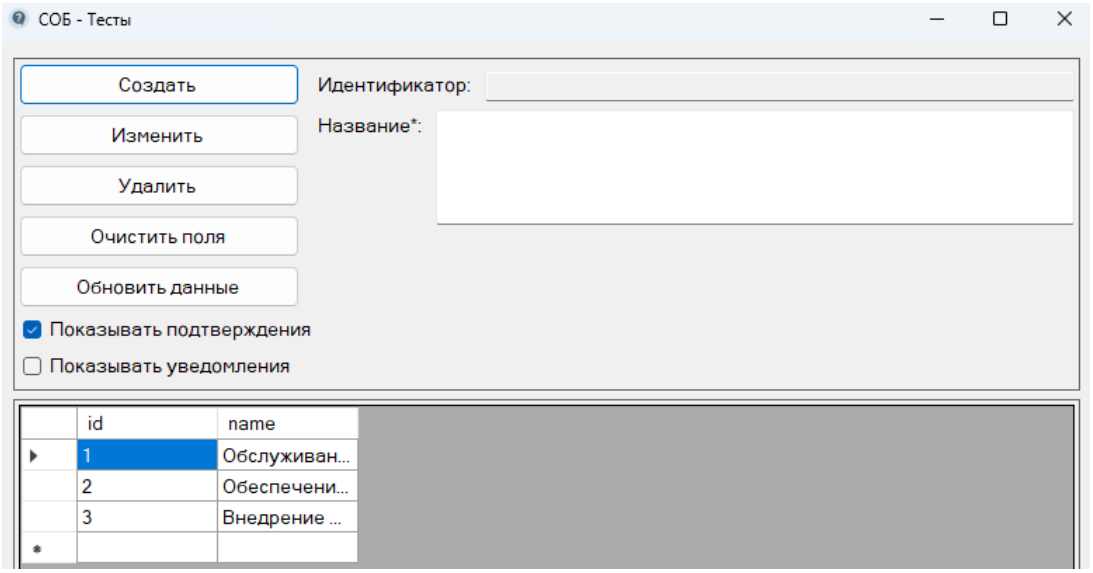

Рисунок 22 — Форма управления тестами

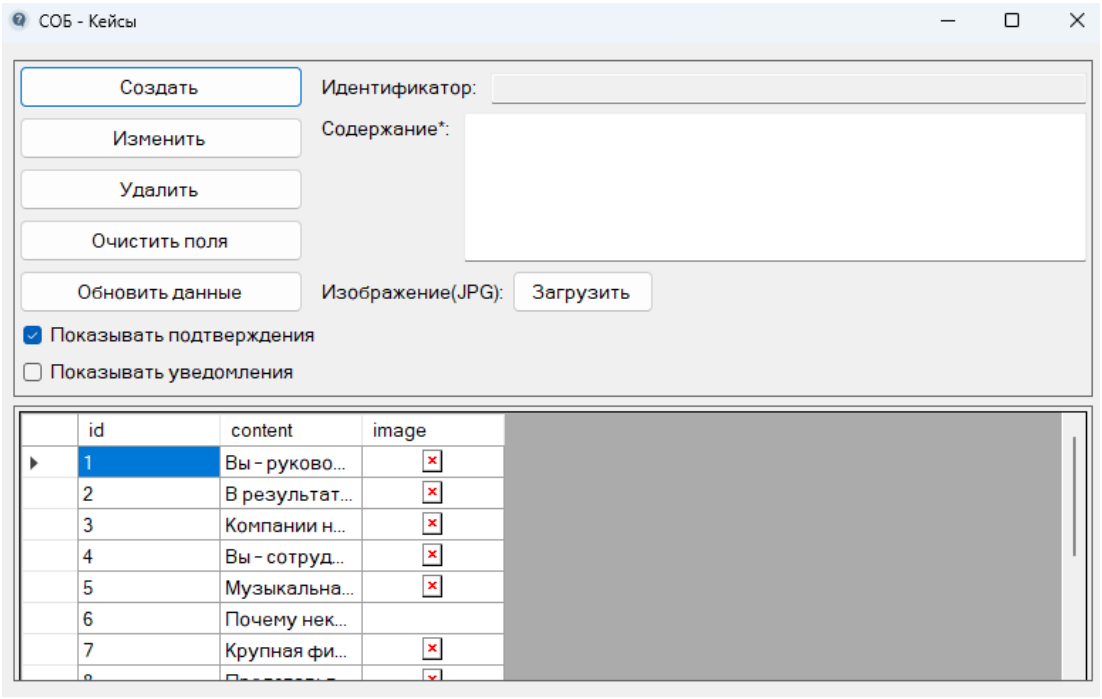

Рисунок 23 — Форма управления кейс-тестами

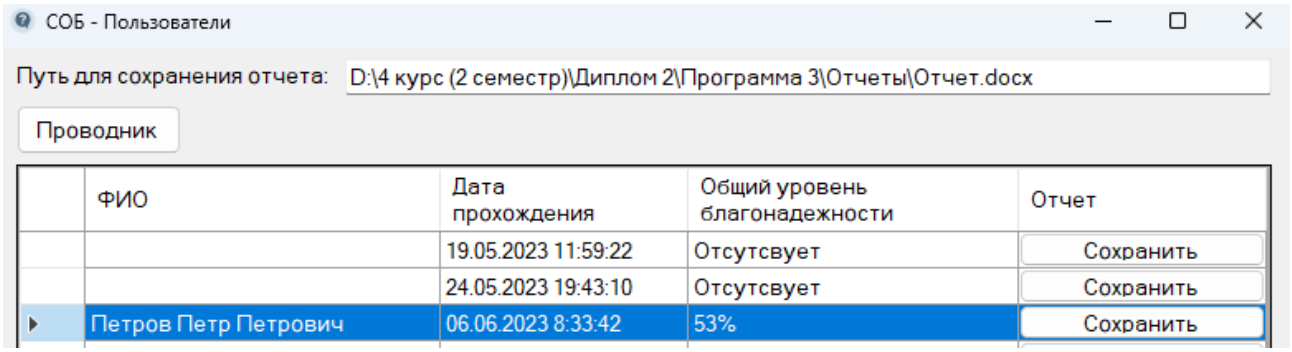

Рисунок 24 — Форма генерации отчета

Модуль тестирования и оценки отвечает за проведение профессионального тестирования кандидатов и оценку их результатов:

Проведение профессионального тестирования – кандидаты могут пройти тесты и кейс-тестирование через пользовательский интерфейс системы.

Отображение промежуточных результатов:

Во время прохождения тестирования, модуль отображает промежуточные результаты, включая количество правильных ответов, выбранных кандидатом.

Кандидаты могут видеть свой текущий прогресс и оценивать свою эффективность в прохождении тестов.

Личностное тестирование:

Модуль тестирования и оценки интегрирует инструменты для проведения личностного тестирования, такие как MMPI (Minnesota Multiphasic Personality Inventory).

Кандидаты могут пройти личностное тестирование, и результаты оценки их личностных качеств будут отображаться в системе.

Данный модуль играет важную роль в процессе оценки кандидатов и позволяет работодателям получить информацию о профессиональных навыках и личностных качествах кандидатов для принятия решений о найме соискателей.

Реализация описанного модуля происходит через классы «Case.cs», «DataBase.cs», «Test.cs» и др., а также через формы, представленные на рисунках 25 – 29.

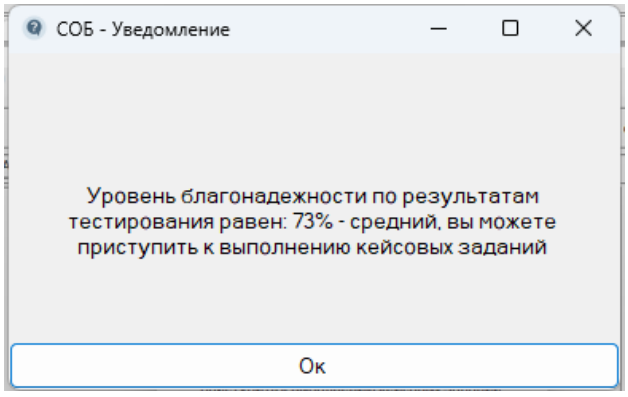

Рисунок 25 — Форма вывода промежуточного результата

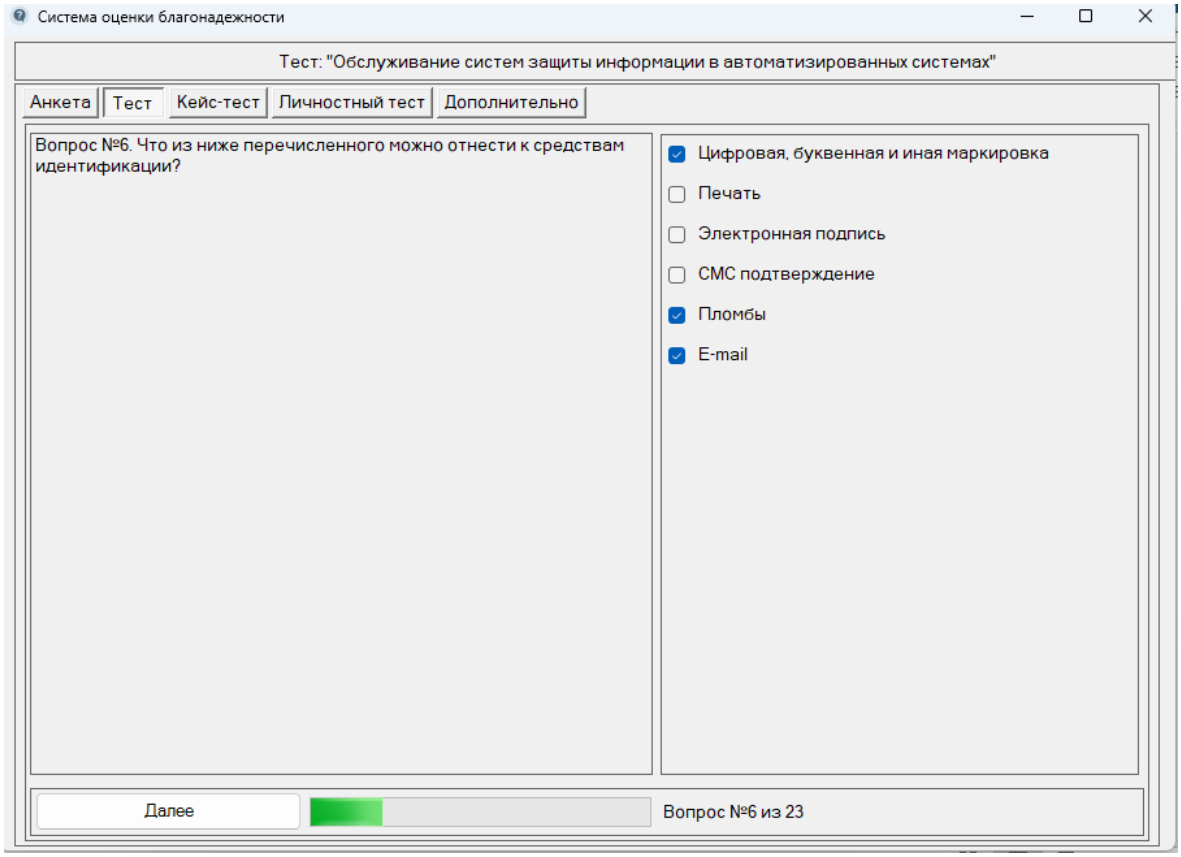

Рисунок 26 — Форма тестирования

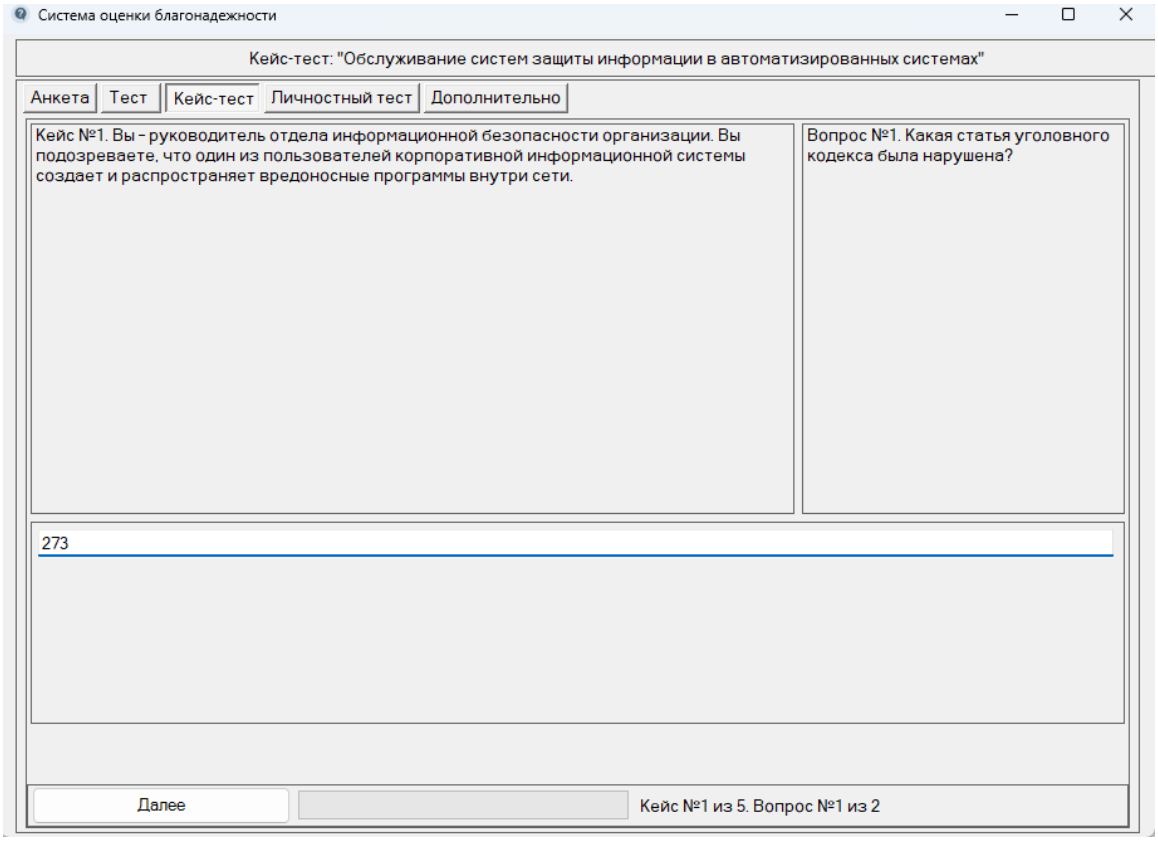

Рисунок 27 — Форма кейс-тестирования

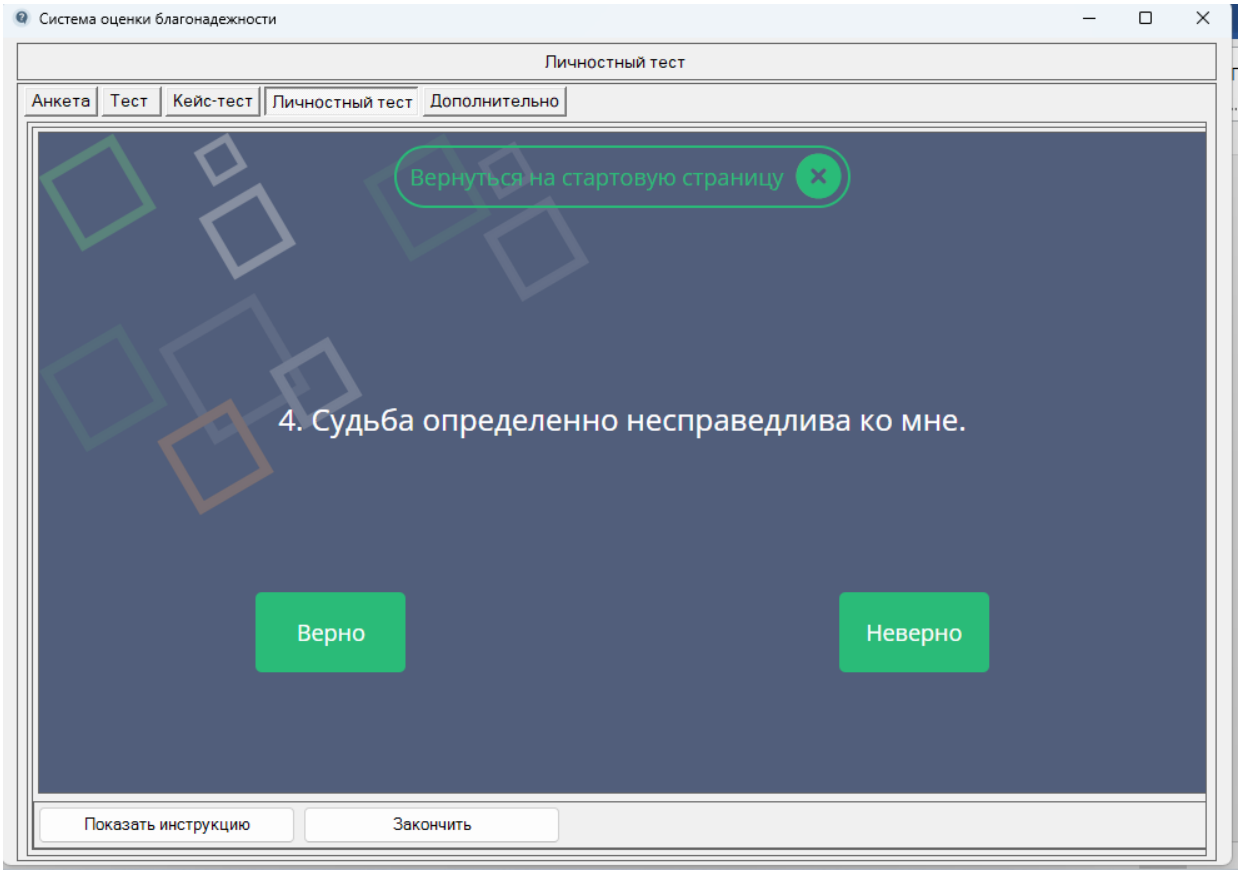

Рисунок 28 — Форма личностного теста

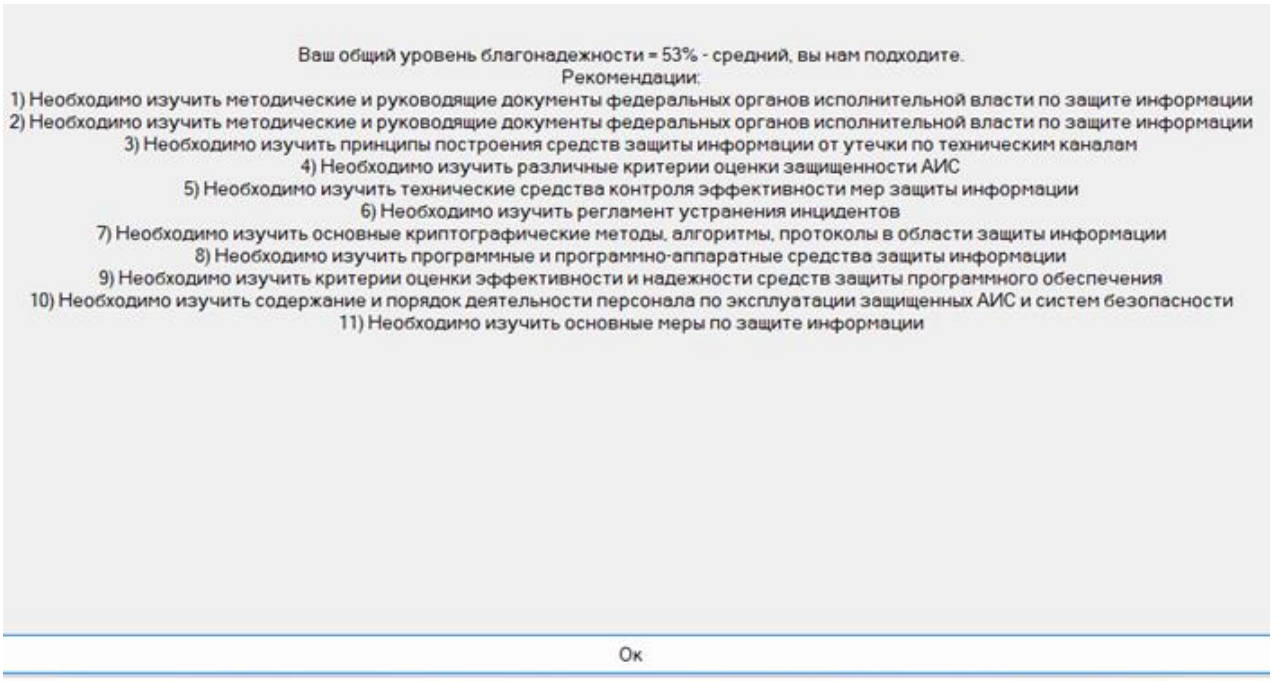

Рисунок 29 — Форма вывода конечного результата

Модуль анкетирования предоставляет возможность проведения опросов и сбора информации от кандидатов:

Создание анкет – система предоставляет различные типы вопросов, такие как выбор из выпадающего списка и текстовое поле ввода данных, для сбора разнообразной информации.

Задание вопросов – вопросы ориентированы на различные аспекты, такие как личные данные, образование, опыт работы, навыки и т.д.

Ответы кандидатов:

– кандидаты могут заполнять анкеты через пользовательский интерфейс системы;

– модуль анкетирования позволяет кандидатам выбирать соответствующие варианты ответов или вводить текстовые данные.

Сбор и обработка информации:

– модуль анкетирования собирает ответы кандидатов и сохраняет их в базе данных для последующей обработки;

– работодатели могут просматривать и анализировать ответы, полученные от кандидатов, с использованием соответствующих функций системы.

Данный модуль реализуется через класс «DataFile.cs», который представлен на рисунке 18 и форму, изображенную на рисунке 30.

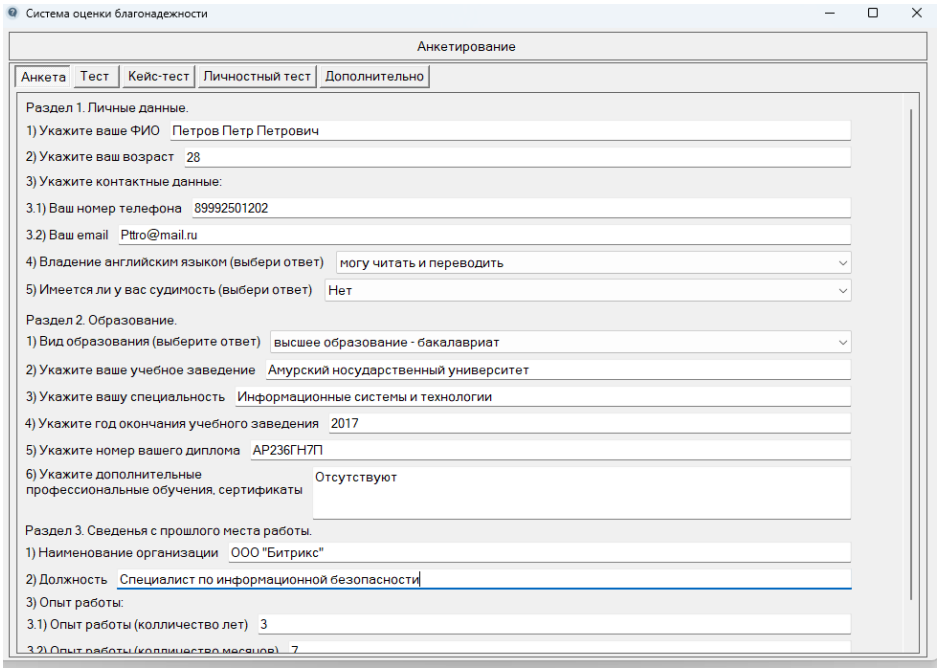

Рисунок 30 — Форма анкетирования

Каждый модуль имеет свою уникальную функциональность и взаимодействует с другими модулями, обеспечивая интегрированную работу системы в целом. Вместе разработанные модули создают полноценное функционирование программного продукта, предоставляя необходимые возможности для эффективного управления и оценки кандидатов.

3.2 Обзор общего алгоритма работы программного продукта

Как уже было описано выше, главная задача разработанного приложения – это оценка кандидата по его профессиональным и личностным качествам.

Основная работа информационного продукта основывается на том, что система считывает ответы соискателя на поставленные вопросы и при помощи эталонных критериев определяет какое количество ответов верно или следует норме, после чего рассчитывается количественный уровень благонадежности в процентном соотношении и выдаются рекомендации о том, следует ли соискателя принимать на работу.

В анкете главными составляющими влияющими на уровень благонадежности являются:

– уровень образования;

– опыт работы;

– владение английским языком.

На основе этих данных определяется какой сложности кандидат будет проходить тестирование и кейс-тестирование.

Следующий этап – решение теста. Для того, чтобы получить одобрение системы перехода на следующий уровень необходимо дать 60 % правильных ответов. Вопросы, содержащиеся в тесте, ранжируются от простых к более сложным и разделены по темам.

После идет уровень решения кейс-тестов, на котором также необходимо набрать 60 % правильных ответов.

И заключительный этап – прохождение личностного теста. На данной ступени необходимо дать ответы на 200 вопросов, которые определяют личные качества кандидата. После завершения данного раздела система выдает общий

уровень благонадежности соискателя. Если уровень оказывается низким, то система сообщает об этом и выдает решение о том, что данного человека нельзя принимать на работу. Если же уровень находится в рамках «средний – высокий», то тогда программа говорит о том, что данного кандидат можно принять на вакантную должность.

Также по окончании оценочного тестирования информационная система выдает рекомендации о том, что соискателю необходимо изучить для повышения своих квалификационных навыков. Темы для рекомендаций система подбирает на основе неправильно данных ответов.

Поэтапный алгоритм работы программного продукта можно рассмотреть на рисунке 31.

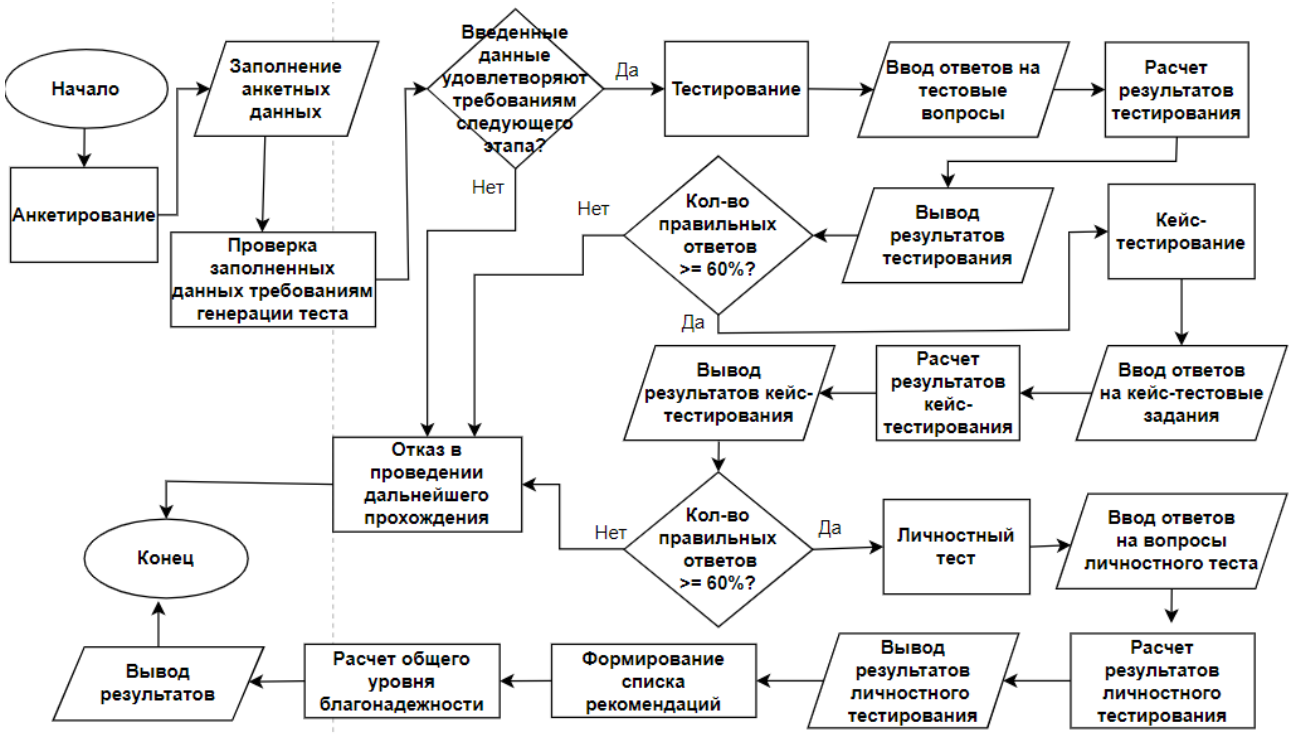

Рисунок 31 — Алгоритм работы программного продукта

Реализация программного продукта является ключевым этапом в создании успешного решения, где абстрактные концепции преобразуются в конкретный функционал. Также в приложении Б, приложении В и приложении Г представлены примеры вопросов, содержащиеся в анкете, тестах и кейс-тестах соответственно.

4 БЕЗОПАСНОСТЬ И ЭКОЛОГИЧНОСТЬ

4.1 Безопасность

4.1.2 Организация рабочего места

Для обеспечения комфортного рабочего места следует учитывать следующие аспекты [21]:

Идеальная высота рабочей столешницы с учетом возможности регулирования составляет от 680 до 800 мм. Уровень высоты составляет 725 мм, если нет возможности настройки разной фиксации. Рабочая поверхность стола должна быть достаточно просторной для размещения компьютера или ноутбука, клавиатуры, мыши и других необходимых инструментов.

Важно обеспечить достаточное пространство для ног под столом. Минимальная высота свободного пространства должна быть не менее 600 мм, ширина не менее 500 мм, а глубина на уровне колен не менее 450 мм и на уровне вытянутых ног не менее 650 мм.

Кресло, на котором будет работать пользователь, должно быть эргономичным и поддерживать правильное положение спины. Ширина и глубина сиденья должны быть не менее 400 мм, передний край сиденья должен быть закруглен и регулируемый в пределах (400-550) мм с углом наклона вперед до 15 градусов и назад до 5 градусов. Угол наклона спинки должен быть в пределах (±30) градусов в вертикальной плоскости.

Если кресло оснащено подлокотниками, они должны быть длиной не менее 250 мм и шириной от 50 до 70 мм. Высота подлокотников должна регулироваться над сиденьем в пределах (230 ± 30) мм, а расстояние между внутренними частями подлокотников должно быть в пределах (350-500) мм.

Изучив выше представленные факты, было выявлено, что рабочие места в ЦИТС и ЗИ МВД имеют некоторые отклонения.

Высота рабочей поверхности составляет 850 мм и не имеет возможности регулировки. Данную проблему можно решить заменой инвентаря либо же

прибегнуть к уменьшению высоты стола путем подпиливания ножек.

Также не совпадает глубина на уровне вытянутых ног из-за присутствия рабочих элементов (удлинители, бесперебойники и др.) под рабочей поверхностью. Решить сложившуюся ситуацию можно правильным распределением элементов оргтехники.

4.1.3 Освещение

Правильное освещение играет важную роль в комфорте и производительности работы с программным продуктом на ЭВМ. Вот несколько особенностей [2]:

Если возможно, необходимо выбирать рабочее место рядом с окном или источником естественного света. Натуральное освещение способствует улучшению настроения и снижению утомляемости. Идеально, если площадь окон составляет около 20 % от площади пола. Коэффициент естественной освещенности должен быть не менее 1,5 % в зависимости от времени года и широты местности.

Дополнительное искусственное освещение должно быть равномерным и без ярких бликов на экране компьютера. Рекомендуется использовать светодиодные или люминесцентные лампы с цветовой температурой около (4000-5000) К, что соответствует естественному свету дневного освещения.

Оптимальный уровень освещенности на рабочей поверхности составляет примерно (500-750) люксов. Для чтения документов или работы с деталями, требующими высокой точности, рекомендуется повысить уровень освещенности до 1000 люксов.

Предпочтительнее использовать настольную лампу с покрывающим абажуром или потолочные светильники, направленные к потолку или стенам, чтобы обеспечить равномерное освещение.

В данной подглаве также замечаются отклонения рабочего места отдела ЦИТС и ЗИ от нормы.

Таким образом всего одно рабочее место расположено около оконного

проема и данный проем не составляет 20 % от площади пола. Так как помещение имеет узкую прямоугольную форму расположить все 4 рабочих места возле окна физически не получится. Данную ситуацию можно разрешить тем, что если есть такая возможность, то для отдела ЦИТС и ЗИ необходимо выделить еще одно помещение.

4.1.4 Шум

При использовании ИС желательно создать тихую рабочую среду, чтобы минимизировать отвлекающие звуки и обеспечить концентрацию, согласно ГОСТ Р 50923-96:

Необходимо разместить рабочее место в тихом углу помещения или использовать шумопоглощающие материалы, такие как ковры или шторы, чтобы снизить проникновение внешних шумов. Оптимальный уровень шума на рабочем месте должен быть менее 55 дБА.

Если вокруг присутствует постоянный шум, можно использовать наушники с шумоподавлением для создания тишины и сосредоточенности.

При выборе компьютера, клавиатуры, мыши и других устройств стоит обратить внимание на их уровень шума. Лучше использовать бесшумные или низкошумные устройства.

Данный раздел имеет особый факт: все сотрудники отдела ЦИТС и ЗИ в начале рабочего дня должны быть подключены к видеоконференцсвязи (ВКС) и слушать вещание. Описанное условие является частью рабочего процесса, которое нельзя пропустить или поставить в бесшумный режим, но звук можно настроить таким образом, чтобы он как можно меньше отвлекал от рабочих задач.

4.1.5 Микроклимат

Поддержание комфортного микроклимата также важно для эффективной работы. Рекомендации включают:

– оптимальная температура в помещении, где установлен компьютер, составляет примерно (20-24) °C;

– оптимальный уровень влажности в помещении равен примерно (40-60) %. Необходимо использовать увлажнители или осушители воздуха, если влажность выше или ниже данного диапазона;

– открывайте окна или используйте вентиляторы для поддержания хорошего воздухообмена.

Нарушений в данном разделе не обнаружено.

4.1.6 Графический интерфейс приложения:

Графический интерфейс приложения имеет важное значение для удобства и эффективности работы пользователей:

– интерфейс должен быть интуитивно понятным и легким в использовании. Необходимо разместить элементы управления и функции таким образом, чтобы они были легко доступны и понятны для каждого пользователя;

– необходимо применять приятную для глаз цветовую схему, которая не вызывает утомления и позволяет легко воспринимать информацию на экране. Желательна возможность настройки цветовых параметров для пользователей с особыми потребностями;

– размер и расположение элементов скина должны быть достаточно большими и удобными для нажатия или выбора с помощью мыши или сенсорного экрана;

– интерфейс должен быть отзывчивым и быстродействующим, чтобы пользователи могли мгновенно взаимодействовать с приложением и получать оперативную обратную связь на свои действия.

Разработанное ПО соответствует выше определенным требованиям, убедиться в этом можно рассмотрев скриншоты приложения, представленные в разделе 3.1.

4.2 Экологичность

4.2.1 Утилизация оргтехники

Утилизация оргтехники в Министерстве внутренних дел проходит в несколько этапов, с соблюдением соответствующих процедур и стандартов.

Перед утилизацией каждое устройство проходит осмотр для определения его состояния. Если оргтехника исправна и подлежит восстановлению или переиспользованию, то она может быть направлена на ремонт или передана другим подразделениям МВД для дальнейшего использования. Если устройство неисправно, оно признается непригодным для использования и подлежит утилизации.

Непригодные для использования оргтехнические устройства собираются и отделяются от рабочих мест. Возможно использование специальных контейнеров или зон, предназначенных для временного хранения отходов.

Каждое устройство, предназначенное для утилизации, оформляется в соответствующих документах, таких как акт утилизации, который содержит информацию о типе устройства, его модели, серийном номере и состоянии.

Непригодные для использования оргтехнические устройства передаются на специализированное предприятие или сертифицированную организацию, занимающуюся утилизацией электронных отходов.

После завершения процесса утилизации оргтехники составляется соответствующая документация, которая подтверждает факт и способ утилизации каждого устройства.

4.2.2 Утилизация макулатуры

Процесс утилизации макулатуры в МВД представлен следующим образом:

– сначала осуществляется систематический сбор макулатуры со всех рабочих мест и офисных помещений. Кипа включает использованные бумажные документы, отчеты, письма, а также бумажные упаковки и коробки. После сбора бумага классифицируется в соответствии с ее типом и качеством, например, разделяется на газетную, офсетную бумагу или гофрированный картон;

– собранная и классифицированная макулатура подвергается подготовке к утилизации. То есть включает в себя удаление скрепок, скоб, пластиковых

элементов или любых других материалов, несовместимых с утилизацией бумаги;

– макулатура, подготовленная к утилизации, передается на специализированные предприятия или перерабатывающие центры.

4.2.3 Утилизация офисной мебели

Процесс утилизации офисной мебели в Министерстве внутренних дел представлен следующим образом:

– перед утилизацией офисная мебель оценивается на предмет ее состояния. В зависимости от состояния, мебель может быть классифицирована как пригодная для переиспользования, требующая ремонта или непригодная для дальнейшего использования;

– если мебель находится в хорошем состоянии или требует только незначительного ремонта, МВД может решить переиспользовать ее внутри организации. Например, мебель может быть передана другим подразделениям или организациям, для которых она будет полезна. В случае необходимости ремонта, производится оценка стоимости ремонтных работ и решается, целесообразно ли их провести;

– если мебель непригодна для переиспользования или ремонта, процедура утилизации включает следующие шаги:

– мебель разбирается на отдельные компоненты и элементы для более эффективной утилизации. Например, деревянные элементы могут быть отделены от металлических или пластиковых;

– компоненты мебели сортируются и классифицируются в соответствии с их типом материала;

– каждый тип материала подвергается переработке, чтобы быть использованным в новых продуктах или материалах;

– любые остатки или неиспользуемые материалы, которые не могут быть переработаны, утилизируются в соответствии с экологическими стандартами и законодательством.

– весь процесс утилизации офисной мебели сопровождается документацией и отчетностью, что включает учет и классификацию мебели, фиксацию проведенных процедур и результатов, а также соблюдение требований по охране окружающей среды и обращению с отходами.

4.2.4 Утилизация люминесцентных ламп

Порядок утилизации следующий:

– люминесцентные лампы, которые нуждаются в утилизации, собираются в специальные контейнеры или установки для сбора отходов. Лампы классифицируются на две категории: истекшие по сроку годности и исправные, которые больше не требуются;

– во время сбора и обработки люминесцентных ламп применяются меры безопасности для предотвращения риска контакта с ртутью;

– и в заключении контейнеры с лампами передаются в специализированные организации, занимающиеся устранением ртутьсодержащих отходов.

4.3 Чрезвычайные ситуации

4.3.1 Пожар

Согласно НПБ 105-03, помещения с ЭВМ являются пожароопасными в категории В1 – В4, в которых могут содержатся материалы, способные гореть при взаимодействии с водой или друг другом.

Для предупреждения и ликвидации такой чрезвычайной ситуации (ЧС) в организации предусмотрены следующие меры:

– установлена и поддерживаться работоспособная система пожарной безопасности, которая включает в себя автоматическую пожарную сигнализацию, систему пожаротушения (огнетушители, пожарные краны и др.), систему дымоудаления;

– имеется разработанный план пожарного режима, включающий организацию путей эвакуации и инструкции по поведению в случае пожара;

– проводятся регулярные тренировки и учения по эвакуации для обучения

персонала действиям в случае ЧС;

– отмечается применение огнестойких строительных материалов, электрических проводов и кабелей;

– системы пожарной безопасности, оборудование и материалы проходят регулярные проверки, обслуживание и испытания для поддержания их работоспособности и соответствия стандартам безопасности;

– поддерживается тесное сотрудничество с местной пожарной службой, что представляет собой проведение совместных учений, обмен информацией о планах пожарной безопасности и консультаций по безопасности.

4.3.2 Террористический акт

В Российской Федерации основным законодательным актом в области противодействия терроризму является Федеральный закон от 6 марта 2006 года № 35 «О противодействии терроризму». Этот закон устанавливает меры по обеспечению безопасности объектов, включая государственные организации и их здания, от террористических угроз.

Кроме того, в России существует Федеральный закон от 26 июня 2008 года № 149 «Об объектах критической информационной инфраструктуры Российской Федерации», который определяет объекты критической информационной инфраструктуры, включая информационные системы и сети, в которые может входить и здание МВД. Этот закон устанавливает требования по обеспечению и защите критической информационной инфраструктуры от угроз и атак, включая террористические.

Для предупреждения и ликвидации террористического акта, МВД предпринимает следующие меры:

– разрабатывает и реализует планы усиления безопасности своих зданий и территорий посредством установки систем видеонаблюдения, контроля доступа, ограждений, пропускных пунктов и дополнительных барьеров для предотвращения несанкционированного проникновения;

– ведёт анализ возможных угроз и разрабатывает стратегии по их

предупреждению и контролю, путем мониторинга деятельности подозрительных группировок или лиц, сотрудничества с разведывательными службами и обмен информацией с другими правоохранительными органами;

– сотрудники МВД проходят обучение по антитеррористической безопасности, распознаванию подозрительных объектов и поведения в экстремальных ситуациях;

– проводятся тренировки по эвакуации, обращению с подозрительными посылками и взрывными устройствами;

– МВД активно сотрудничает с другими правоохранительными органами, спецслужбами и органами безопасности для обмена информацией, координации действий и обеспечения оперативного реагирования на возможные угрозы;

– в случае возникновения террористической угрозы или нападения, МВД формирует оперативные группы и штабы для координации действий, принятия оперативных решений и обеспечения эффективной реакции на ЧС;

– организация оснащает свои подразделения специальным оборудованием и техникой для нейтрализации террористических угроз и обеспечения безопасности при проведении специальных операций.

ЗАКЛЮЧЕНИЕ

В ходе выполнения данного дипломного проекта была разработана информационная система оценки уровня благонадежности соискателя на должность специалиста по защите информации. Процесс разработки системы включал анализ предметной области, проектирование ИС, разработку тестов и кейс-тестов, описание функциональных блоков системы, а также анализ инструментальных средств разработки, существующих решений и аспектов безопасности и экологичности работы.

Анализ предметной области являлся важным этапом работы, поскольку позволил получить полное представление о требованиях и особенностях профессиональной деятельности специалиста по защите информации. Благодаря данному анализу были выявлены основные критерии и параметры, необходимые для оценки благонадежности соискателя на данную вокантную должность.

Следующим шагом было проектирование ИС, которое включало проектирование архитектуры системы, базы данных и методики расчета уровня благонадежности. Важным аспектом проектирования было обеспечение надежности, эффективности и безопасности системы, а также удобства использования для пользователей.

В рамках работы были описаны функциональные блоки системы, определены их основные задачи и функции. Это позволило создать структуру ПО, где каждый блок выполняет определенные действия, взаимодействуя с другими блоками и обеспечивая целостность и эффективность работы системы в целом.

При выборе инструментальных средств разработки проведен анализ различных вариантов с учетом требований проекта. Были выбраны наиболее подходящие инструменты, обладающие необходимыми функциональными возможностями.

В процессе анализа существующих решений было выявлено, что разработанная ИС обладает рядом преимуществ перед аналогами. Она предоставляет более точную и надежную оценку уровня благонадежности соискателя на должность специалиста по защите информации, а также обеспечивает удобство использования и не требует денежных ресурсов.

Особое внимание уделено вопросам безопасности и экологичности работы с ИС. Были применены принципы энергоэффективности и оптимизации ресурсов, чтобы уменьшить негативное влияние на окружающую среду.

Подводя итоги можно сказать о том, что разработка информационной системы оценки уровня благонадежности соискателя на должность специалиста по защите информации была успешно выполнена.

Полученная ИС обладает высокой функциональностью, надежностью, безопасностью и удобством использования. Разработанные тесты и кейс-тесты позволяют проводить качественную оценку соискателей.

В результате данного проекта были достигнуты поставленные цели и получены положительные результаты.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1 Благодаров, А. В. Клиент-серверные приложения баз данных : учебное пособие / А. В. Благодаров, Н. Н. Гринченко, А. Ю. Громов. — Рязань. : РГРТУ, 2018. – 72 с.

2 Булгаков, А. Б. Безопасность жизнедеятельности [Электронный ресурс] : сб. учеб.-метод. материалов / АмГУ, ИФФ ; сост.: А. Б. Булгаков, В. Н. Аверьянов, М. В. Гриценко. – Благовещенск : Изд-во Амур. гос. ун-та, 2017. – 176 с. – Б. ц.

3 Глухарева, С. В. Методика подбора персонала на должности, связанные с обработкой конфиденциальной информации / С. В. Глухарева. – Екатеринбург. : Изд-во Урал. ун-та, 2018. – С. 154-158.

4 Йордон, Э. Путь камикадзе. Как разработчику программного обеспечения выжить в безнадежном проекте / Э. Йордон. – М. : ЛОРИ, 2018. – 255 с.

5 Кардаш, Т. А. Эргономика рабочих мест служащих и инженерно-технических работников, оснащенных ПЭВМ [Текст] : учеб. пособие / Т. А. Кардаш ; АмГУ, ИФФ. – Благовещенск : Изд-во Амур. гос. ун-та, 2002. – 60 с.

6 Карпова, И. П. Проектирование реляционной базы данных: Метод. указания к домашнему заданию по курсу «Базы данных» / И. П. Карпова. – Москва : Изд-во Моск. ин-та электроники и математики им. А.Н. Тихонова; 2018. – 29 с.

7 Костюк, А. И. Администрирование баз данных и компьютерных сетей : учеб. пособие / А. И. Костюк, Д. А. Беспалов. – Ростов-на-Дону. : ЮФУ, 2020. – 127 с.

8 Москвитин А. А. Данные, информация, знания: методология, теория, технологии / А. А. Москвитин. – Изд-во Лань, 2019− 236 с.

9 Николаев, Д. А. Комплексная проверка сотрудников на благонадежность как превентивный механизм противодействия корпоративному мошенничеству в кредитных организациях [Электронный

ресурс] / Д. А. Николаев, К. Н. Сургутанова. – 2020. – № 12 (302). – С. 122-125. – Режим доступа : https://moluch.ru/archive/302/68287/. – 16.02.2023.

10 Озкайя, Э. Кибербезопасность. Стратегии атак и обороны / Ю. Диогенес, Э. Озкайя. – М. : ДМК Пресс, 2020. – 326 с.

11 Профстандарт № 06.033. Специалист по защите информации в автоматизированных системах [Электронный ресурс] / МИНТРУД РОССИ. – Утвер. 14.09.2022. – Режим доступа : https://classinform.ru/profstandarty/06.033-spetcialist-po-zashchite-informatcii-v-avtomatizirovannykh-sistemakh.html. – 01.02.2023.

12 Приказ № 774н «Об утверждении общих требований к организации безопасного рабочего места» [Электронный ресурс] / МИНТРУД РОССИ И СОЦИАЛЬНОЙ ЗАЩИТЫ РФ. – Утвер. 29.10.2021. – Режим доступа : http://publication.pravo.gov.ru/Document/View/0001202111250035. – 19.05.2023

13 Стандарт организации. Оформление выпускных квалификационных и курсовых работ (проектов) [Электронный ресурс] / АмГУ ; разраб. Л. А. Проказина, Н. А. Чалкина, С. Г. Самохвалова. – Введ. с 05.04.2018. – Благовещенск : [б. и.], 2018. – 75 с. Режим доступа : https://irbis.amursu.ru/DigitalLibrary/AmurSU_Edition/9702.pdf. – 07.03.2023.

14 Троелсен, Э. Язык программирования C# 9 и платформа .NET 5: основные принципы и практики программирования / Ф. Джепикс, Э. Троелсен. – М. : Диалектика (Вильямс), 2022. – 1392 с.

15 Тузовский, А.Ф. Объектно-ориентированное программирование: учебное пособие для прикладного бакалавриата / А. Ф. Тузовский. – Москва: Из-дательство Юрайт, 2019. – 206 с. – (Университеты России). – ISBN 978-5-534-00849-4. – Текст: электронный // ЭБС Юрайт [сайт]. – URL: https://biblio-online.ru/bcode/434045 (дата обращения: 02.05.2023).

16 УМВД по Амурской области - МВД России: Структура [Сайт]. – 2023. Режим доступа : https://28.xn--b1aew.xn--p1ai/.– 12.05.2023.

17 Федеральный закон № 149 «Об информации, информационных технологиях и о защите информации» [Электронный ресурс] / Гос. Дума ФС

РФ. – Утвер. 27. 07. 2006. – Режим доступа: https://www.consultant.ru/document/cons_doc_LAW_61798/. – 08.05.2023.

18 Хабр Q&A: Программное обеспечение и интернет-сервисы методологии разработки [Сайт]. – 2020. – Режим доступа : https://qna.habr.com/q/174615. – 20.01.2023.

19 Черёмушкин А. В. Криптографические протоколы: основные свойства и уязвимости : научная статья / А. В. Черёмушкин. – Москва : Институт криптографии, связи и информатики, 2009. – 36 с.

20 Шелупанов, А. А. Оценка благонадежности сотрудника в системе кадровой безопасности предприятия / С. В. Глухарева, М. М. Немирович-Данченко, А. А. Шелупанов. – Томск : Изд-во Томского гос. ун-та систем управления и радиоэлектроники, 2021. – № 4. – С. 52-57

21 Шумилин, В. К. Пособие по безопасной работе на персональных компьютерах [Текст] / разраб. Шумилин. – М. : НЦ ЭНАС, 2005. – 28 с.

22 Microsoft : Добро пожаловать в интегрированную среду разработки Visual Studio [Сайт]. – 25.05.2023. – Режим доступа : https://learn.microsoft.com/ru-ru/visualstudio/get-started/visual-studio-ide?view=vs-2022. – 28.02.2023.

23 Otus journal: Информационная безопасность от А до Я [Электронный ресурс]. – 11.01.2023. – Режим доступа : https://otus.ru/journal/informacionnaya-bezopasnost-ot-a-do-ya/. – 12.04.2023

24 Segal, E. 25% Of Workers Lost Their Jobs In The Past 12 Months After Making Cybersecurity Mistakes: Report [Электронный ресурс] / E. Segal. – 2022. – Режим доступа : https://www.forbes.com/sites/edwardsegal/2022/03/29/25-of-workers-lost-their-jobs-in-the-past-12-months-after-making-cybersecurity-mistakes-report/?sh=6ce8604049b2. – 10.10.2022.

25 Zheguang, Z. Encrypted Databases: From Theory to Systems / S. Kamara, T. Moataz, S. Zdonik. – Chaminade, 2021. – 7 c.

ПРИЛОЖЕНИЕ А

Техническое задание на разработку программного продукта

1. Общие сведенья

1.1. Наименование системы

Информационная система «Оценки уровня благонадежности соискателя на должность специалиста по защите информации».

1.1.2. Краткое наименование системы

ИС «RAS»

1.2. Краткая характеристика области применения программы

Информационная система предназначена для дачи качественной оценки имеющихся личностных и профессиональных компетенций претендентов на должность специалиста по защите информации в соответствии с профстандартом № 06.033.

1.3. Основание для проведения разработки

Основанием для разработки служит задание к выпускной квалификационной работе.

1.3.1. Исполнитель

Студентка 4 курса ФГБОУ ВО АмГУ Панасюк Дарья Владимировна

1.4. Плановые сроки начала и окончания работы

Начало работ: 01.10.2022

Срок окончания работ: 03.06.2023

1.5. Порядок оформления и предъявления результатов работ

Результатом работы является разработанная информационная система и пояснительная записка к ней, оформленная по стандарту АмГУ в рамках дипломного проекта. С 01.05.23 по 20.05.23 показывается первая часть работы — пояснительная записка с описанием предметной области и основных информационных объектов, участвующих в разработке ИС. С 20.05.23 по 03.06.23 предъявляется готовый разработанный информационный продукт руководителю проекта.

2. Назначение и цели создания системы

2.1. Назначение

ИС предназначена для обеспечения кадровой безопасности предприятия путем правильно подобранных благонадежных кадров, обладающих требуемыми компетенциями.

2.2. Цели создания системы

2.2.1. С точки зрения создателей системы:

– Построить платформу для интерактивного общения соискателей и организации.

– Продемонстрировать навыки полученные в рамках обучения через выпускное квалификационное проектирование.

2.2.2. С точки зрения организации:

– Снизить трудозатраты и настроить четкую и удобную организацию проведения собеседования соискателей.

– Ускорить процесс проведения собеседования за счет нового продукта.

– Увеличить уровень квалифицированных кадров за счет появления новой системы проверки уровня квалификации.

2.2.3. С точки зрения соискателей:

– Получить возможность более объективной оценки.

– Повысить комфортность проведения собеседования.

3. Характеристика объектов автоматизации

Объектом автоматизации является процесс подбора персонала на вакантную должность.

3.1 Существующее программное обеспечение

В настоящий момент в ГУМВД при найме сотрудников используются следующие объекты:

– полиграф;

– единая база данных, содержащая информацию о гражданах, включая паспортные данные, регистрацию места жительства, фотографии, сведения

о семейном положении и другие персональные данные;

– регистр судимостей и др.

3.2. Описание процессов ГУМВД

3.2.1 Процесс подбора сотрудника на работу

В таблице А.1 представлен процесс подбора сотрудника как государственного служащего, а в таблице А.2 как гражданского служащего.

Таблица А.1 — Процесс подбора сотрудника на работу как государственного служащего

Этапы трудоустройства	Описание
Подача заявления	Соискатель подает заявление и предоставляет необходимые документы.
Проверка документов	МВД проверяет предоставленные документы и их подлинность.
Медицинское обследование	Кандидаты проходят медицинское обследование для установления их физической годности к службе.
Проверка физической подготовки	Соискатели сдают нормативы по физической подготовки
Полиграф	Прохождение полиграфического тестирования для проверки достоверности предоставленной информации.
Собеседование	Соискатели проходят собеседование с представителями МВД для оценки их навыков, мотивации и соответствия требованиям должности.
Решение о приеме	На основе результатов всех этапов, МВД принимает решение о приеме соискателя на должность государственного служащего.

Таблица А.2 — Процесс подбора сотрудника на работу как гражданского служащего

Этапы трудоустройства	Описание
Подача заявления	Соискатель подает заявление и предоставляет необходимые документы.
Проверка документов	МВД проверяет предоставленные документы и их подлинность.
Медицинское обследование	Кандидаты проходят мед. обследование для установления их физической годности к службе.

Продолжение таблицы А.2

Собеседование	Соискатели проходят собеседование с представителями МВД для оценки их навыков, мотивации и соответствия требованиям должности.
Решение о приеме	На основе результатов всех этапов, МВД принимает решение о приеме соискателя на должность гражданского служащего.

4. Требования к системе

4.1. Требования к системе в целом

4.1.1. Требования к структуре и функционированию системы

4.1.1.1 Перечень подсистем, их назначение и основные характеристики

В состав ИС должны входить следующие подсистемы:

– Подсистема хранения данных;

– Подсистема анализа;

– Подсистема математической обработки данных;

– Подсистема формирования отчетности.

Подсистема хранения данных предназначена для хранения оперативных данных системы, сведений для формирования аналитических отчетов.

Подсистема анализа предназначена для аналитической обработки накопленного массива данных ИС.

Подсистема математической обработки данных предназначена для построения процентной модели исследуемого процесса определения уровня благонадежности на основе конечной выборочной совокупности предоставленных данных.

Подсистема формирования отчетности предназначена для создания и формирования отчетов в виде удобном для вывода на печатающие устройства на основе данных ИС «RAS».

4.1.2. Требования к численности и квалификации персонала системы

Для эксплуатации ИС определены следующие роли:

– системный администратор;

– администратор баз данных;

– пользователь.

Системный администратор должен обладать высоким уровнем квалификации и практическим опытом выполнения работ по установке, настройке и администрированию программных и технических средств, применяемых в системе.

Администратор баз данных должен обладать высоким уровнем квалификации и практическим опытом выполнения работ по установке, настройке и администрированию используемых в АС СУБД.

Пользователи системы должны иметь опыт работы с персональным компьютером на базе операционных систем Microsoft Windows на уровне квалифицированного пользователя и свободно осуществлять базовые операции.

Роли системного администратора и администратора баз данных могут быть совмещены в одну роль.

Рекомендуемая численность для эксплуатации ИС:

Администратор – 1 штатная единица.

Пользователь – число штатных единиц определяется структурой предприятия.

4.1.3. Требования к надежности

Уровень надежности должен достигаться согласованным применением организационных, организационно-технических мероприятий и программно-аппаратных средств.

Надежность должна обеспечиваться за счет:

– применения технических средств, системного и базового программного обеспечения, соответствующих классу решаемых задач;

– своевременного выполнения процессов администрирования системы;

– соблюдения правил эксплуатации и технического обслуживания

программно-аппаратных средств;

– предварительного обучения пользователей и обслуживающего персонала;

– выполнения рекомендаций Министерства труда и социального развития РФ, изложенных в Постановлении от 23 июля 1998 г. «Об утверждении межотраслевых типовых норм времени на работы по сервисному обслуживанию ПЭВМ и оргтехники и сопровождению программных средств».

4.1.4. Требования к защите информации от несанкционированного доступа

Компоненты подсистемы защиты от НСД должны обеспечивать:

– идентификацию пользователя;

– проверку полномочий пользователя при работе с системой;

– разграничение доступа пользователей на уровне задач и информационных массивов.

Защищенность системы обеспечивается путем:

– использования скрытого набора пароля (при наборе пароля его символы не показываются на экране либо заменяются одним типом символов; количество символов не соответствует длине пароля);

– использование разграничения прав доступа;

– использования системы шифрования.

4.2 Требования к видам обеспечения

4.2.1. Требования к математическому обеспечению системы

Математические методы и алгоритмы, используемые для шифрования или дешифрования данных, а также программное обеспечение, реализующее их, должны быть сертифицированы уполномоченными организациями.

4.2.2 Требования к информационному обеспечению системы

4.2.2.1 Требования к составу, структуре и способам организации данных в системе

Состав, структура и способы организации данных в системе должны быть определены на этапе технического проектирования. Уровень хранения данных в системе должен быть построен на основе современных реляционных или объектно-реляционных СУБД. Для обеспечения целостности данных должны использоваться встроенные механизмы СУБД.

4.2.3. Требования к лингвистическому обеспечению системы

При реализации системы должны применяться следующие языки высокого уровня: SQL, C#.

Все прикладное программное обеспечение системы для организации взаимодействия с пользователем должно использовать русский язык.

4.2.4. Требования к программному обеспечению

Используемое при разработке программное обеспечение и библиотеки программных кодов должны иметь широкое распространение, быть общедоступными и использоваться в промышленных масштабах. Базовой программной платформой должна являться операционная система MS Windows.

4.2.5. Требования к техническому обеспечению

Техническое обеспечение системы должно максимально и наиболее эффективным образом использовать существующие в ГУМВД технические средства.

Требования к техническим характеристикам веб-сервера:

– процессор Intel Xeon с тактовой частотой не менее 3 ГГц;

– объем оперативной памяти не менее 16 Гб;

– жесткий диск или массив жестких дисков с общим объемом не менее 500 Гб;

– устройство чтения компакт-дисков (DVD-ROM) или возможность чтения и записи CD/DVD/Blu-ray дисков;

– сетевой адаптер ethernet с поддержкой скорости передачи данных не менее 1 Гбит/с.

Продолжение ПРИЛОЖЕНИЯ А

Требования к техническим характеристикам ПК пользователя и ПК администратора:

– процессор Intel Core i5 или аналогичный с тактовой частотой не менее 2.5 ГГц;

– объем оперативной памяти не менее 4 Гб;

– жесткий диск или SSD с объемом не менее 256 Гб;

– поддержка разрешения экрана не менее 1280x1024 пикселей и цветовой глубины не менее 24 бит/пиксель;

– сетевой адаптер ethernet с поддержкой скорости передачи данных не менее 100 Мбит/с.

5. Состав и содержание работ по созданию системы

Данные приведены в таблице А.3.

Таблица А.3 — Этапы создания системы

Содержание работ	Результаты работ
Предпроектное исследование, сбор необходимой информации.	Определение целей, задач системы, которые в дальнейшем должны быть решены.
Анализ предметной области.	Подробный анализ системы и введение организационных требований к решению задач и целей.
Разработка ТЗ.	Документация на разрабатываемую систему, в которой указаны сроки реализации, кем будет реализована, для кого, описаны все необходимые требования для разработки.
Разработка модели программы.	Описание спецификаций данных, определение связей между сущностями, построение концептуальной модели БД, построение логической модели БД.

Продолжение таблицы А.3

Разработка ТП	–
Разработка рабочего проекта, состоящего из: – написания программы; – отладка программы; – корректировка программы.	–
Проведение тестирования и доработка информационного программного обеспечения по замечаниям и предложениям	–
Сдача системы в эксплуатацию с выпуском описания алгоритмов и технологической документации.	Акт приема сдаточных работ

6. Порядок контроля и приемки системы

6.1. Общие требования к приемке работ по стадиям

Сдача-приёмка работ производится поэтапно, в соответствии с рабочей программой и календарным планом, представленным в таблице А.4.

Таблица А.4 — Календарный план

Наименование этапа	Сроки этапа	Результат выполнения этапа
Изучение предметной области	01.05.2023 – 05.05.2023	Предложения по разработке программного обеспечения. Проектирование системы. Выбор средства реализации. Разработка системы. Акт сдачи – приемки предложений по реализации системы.

Продолжение таблицы А.4

Разработка программного обеспечения	06.05.2023 – 20.05.2023	Завершенный программный комплекс. Внедрение системы.
Тестирование и отладка ПО	21.05.2023 – 03.06.2023	Готовое программное обеспечение.
Разработка программного обеспечения	06.05.2023 – 20.05.2023	Завершенный программный комплекс. Внедрение системы.
Внедрение	04.06.2023 – 19.06.2023	Функционирование системы. Программная документация. Акт сдачи – приёма работ.

7. Требования к составу и содержанию работ по подготовке объекта автоматизации к вводу системы в действие

При подготовке к вводу в эксплуатацию ИС «Оценки уровня благонадежности соискателя на должность специалиста по защите информации» Заказчик должен обеспечить выполнение следующих работ:

– определить подразделение и ответственных должностных лиц, за внедрение и проведение опытной эксплуатации ИС;

– обеспечить присутствие пользователей на обучении работе с системой, проводимой Исполнителем;

– обеспечить соответствие помещений и рабочих мест пользователей системы в соответствии с требованиями, изложенными в настоящем ТЗ;

– обеспечить выполнение требований, предъявляемых к программно-техническим средствам, на которых должно быть развернуто программное обеспечение ИС «Оценки уровня благонадежности соискателя на должность специалиста по защите информации»;

– совместно с Исполнителем подготовить план развертывания системы на технических средствах Заказчика;

– провести опытную эксплуатацию ИС «Оценки уровня благонадежности соискателя на должность специалиста по защите информации».

8. Требования к документированию

Для системы на различных стадиях создания должны быть выпущены документы из числа предусмотренных в ГОСТ 34.201–89 «Информационная технология. Комплекс стандартов на автоматизированные системы».

9. Источники разработки

В настоящем документе использованы следующая литература и нормативные документы:

– ГОСТ 12.2.003 «Система стандартов безопасности труда. Оборудование производственное. Общие требования безопасности»;

– ГОСТ 19.XXX «Единая система программной документации»;

– ГОСТ 19.004-80 «Единая система программной документации. Термины и определения»;

– ГОСТ 19.101-77 «Единая система программной документации. Виды программ и программных документов»;

– ГОСТ 19.102-77 «Единая система программной документации. Стадии разработки»;

– ГОСТ 19.201-78-82 «Единая система программной документации. Техническое задание. Требования к содержанию и оформлению»;

– ГОСТ 21552-84 «Средства вычислительной техники. Общие технические требования, приёмка, методы испытаний, маркировка, упаковка, транспортирование и хранение».

ПРИЛОЖЕНИЕ Б

Пример перечня анкетных вопросов

Раздел 1. Личные данные.

1) Укажите ваше ФИО_____

2) Укажите ваш возраст_____

3) Укажите контактные данные:

- Ваш номер телефона_____
- Ваш email_____

4) Владение английским языком (выбери ответ):

- Могу читать и переводить
- Могу свободно говорить, читать и переводить
- Не владею

5) Имеется ли у вас судимость? (выбери ответ): Да/Нет.

Раздел 2. Образование.

1) Вид образования (выберите ответ):

- Основное общее образование (9 классов)
- Среднее общее образование (11 классов)
- Среднее профессиональное образование (колледж/техникум)
- Высшее образование - бакалавриат
- Высшее образование - специалитет, магистратура

2) Укажите ваше учебное заведение_____

3) Укажите вашу специальность_____

4) Укажите год окончания учебного заведения_____

5) Укажите номер вашего диплома_____

6) Укажите дополнительные профессиональные обучения, сертификаты

Раздел 3. Сведенья с прошлого места работы.

1) Наименование организации_____

2) Должность_____

3) Опыт работы_____

ПРИЛОЖЕНИЕ В

Пример перечня тестовых вопросов

Вопрос 1. Какой из протоколов рассматривается как механизм аутентификации и авторизации удалённых пользователей в условиях распределённой сетевой инфраструктуры, предоставляющий централизованные услуги по проверке подлинности и учёту для служб удалённого доступа?

- PAP (Password Authentication Protocol)
- CHAP (Challenge Handshake Authentication Protocol)
- EAP (Extensible Authentication Protocol)
- RADIUS (Remote Authentication Dial-in User Service)
- TACACS (Terminal Access Controller Access Control System)

Вопрос 2. Какое из перечисленных ниже средств оценки защищенности информации предназначено для контроля подсистемы обеспечения целостности?

- Ревизор 2 XP
- ФИКС
- TERRIER
- Ревизор сети

Вопрос 3. Этот принцип политики информационной безопасности состоит в том, что безопасность не должна обеспечиваться через неясность.

- Контроль над всеми операциями
- Разграничение доступа
- Открытая архитектура ИС
- Запрещено всё, что не разрешено

Вопрос 4. Структура систем защиты должна зависеть от:

- Перечня угроз защищаемой системы
- Механизмов защиты
- Архитектуры

Продолжение ПРИЛОЖЕНИЯ В

Вопрос 4. Соотнесите принцип организации систем защиты и его значение:

а) Принцип превентивности	1. Подразумевает, что средства, затраченные на защиту информации, не должны превышать стоимости информации
б) Принцип экономической целесообразности	2. Содержание этого принципа предполагает своевременное выявление тенденций и предпосылок, способствующих развитию угроз.
в) Принцип обоснованности защиты информации	3. Выполнение этого принципа заключается в установлении путем экспертной оценки целесообразности засекречивания и защиты той или другой информации, вероятных экономических и других последствий такой защиты исходя из баланса жизненно важных интересов государства, общества и граждан

Вопрос 5. О какой мере защиты информации идет речь: Она осуществляет мониторинг внутреннего и внешнего трафика и фиксируется события, связанные с копированием, передачей наружу или выводом на печать конфиденциальной информации.

- Применение DLP-системы
- Применение SIEM-системы
- Архивация данных

ПРИЛОЖЕНИЕ Г

Пример перечня кейс-тестовых заданий

Кейс-тест 1. Вы – руководитель отдела информационной безопасности организации. Вы подозреваете, что один из пользователей корпоративной информационной системы создает и распространяет вредоносные программы внутри сети.

Вопрос 1: Какая статья уголовного кодекса была нарушена?_____

Вопрос 2: Какое наказание должен понести нарушитель? (Соотнесите)

а) Деяния заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ и т. д.	1. Наказываются лишением свободы на срок до трех лет со штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода, осужденного за период до восемнадцати месяцев
б) Те же деяния, повлекшие по неосторожности тяжкие последствия	2. Наказываются лишением свободы на срок от трех до семи лет

Кейс-тест 2. Вы – сотрудник фармацевтического учреждения. Ежедневно в базе данных происходит накопление большого количества информации. Перечислите возможные способы обеспечения целостности и предотвращения уничтожения данных.

Введите ответ со строчной буквы без пробелов через запятую:_____

Кейс-тест 3. Представьте ситуацию, что вы купили новый компьютер. Вы очень часто используете его для общения в социальных сетях, игр в режиме онлайн, переписки по средствам электронной почты, поиска информации.

Укажите, какой/каким угрозе/угрозам больше всего подвержена информация:

- Угроза нарушения конфиденциальности
- Угроза нарушения целостности
- Угроза отказа служб
- Верны все варианты ответа