

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
«Тольяттинский государственный университет»

Институт математики, физики и информационных технологий
(наименование института полностью)

Кафедра «Прикладная математика и информатика»
(наименование)

01.03.02 Прикладная математика и информатика
(код и наименование направления подготовки, специальности)

Компьютерные технологии и математическое моделирование
(направленность (профиль)/специализация)

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА (БАКАЛАВРСКАЯ РАБОТА)

на тему «Компьютерная модель системы контроля и учета электронных цифровых подписей в организации»

Обучающий

А.А. Николенко

(Инициалы Фамилия)

(личная подпись)

Руководитель

к.т.н., доцент, О.М. Гущина

(ученая степень (при наличии), ученое звание (при наличии), Инициалы Фамилия)

Консультант

к.п.н., доцент, Т.С. Якушева

(ученая степень (при наличии), ученое звание (при наличии), Инициалы Фамилия)

Тольятти 2023

Аннотация

Тема бакалаврской работы: «Компьютерная модель системы контроля и учета электронных цифровых подписей в организации».

Бакалаврская работа посвящена разработке компьютерной модели системы контроля и учета электронных цифровых подписей в организации.

В ходе выполнения исследований по бакалаврской работе был проведен анализ существующих решений электронных цифровых подписей, разработка компьютерной модели системы контроля и учета электронных цифровых подписей в организации, проектирование интерфейса и разработка приложения.

Во введении прописывается актуальность темы, написаны цель и задачи.

В первом разделе рассматриваются способы контроля и учета электронных цифровых подписей.

Во втором разделе описывается структурная схема системы и разрабатывается алгоритм работы системы.

Третий раздел содержит описание интерфейса, разработку приложения и тестирование приложения.

В заключении представлены результаты выполнения выпускной квалификационной работы.

Бакалаврской работа состоит из введения, трёх разделов, заключения и списка использованной литературы.

Бакалаврская работа состоит из 41 страниц, 23 рисунков, 25 источников.

Abstract

The title of the bachelor's thesis is "Computer model of the system of control and accounting of electronic digital signatures in the organization".

The research is devoted to development of a computer model of the system of control and accounting of electronic digital signatures in the organization.

When doing a research, the analysis of existing solutions of electronic digital signatures, the development of a computer model of the system of control and accounting of electronic digital signatures in the organization, interface design and application development were carried out.

The introduction reveals the relevance of the research and gives a brief description of the work done.

The first section the methods of control and accounting of electronic digital signatures are considered.

The second section the structural scheme of the system is described and the algorithm of the system is developed.

The third section interface description, application development and application testing.

In conclusion, the conclusions of the entire work are drawn.

The bachelor's thesis consists of an introduction, three sections, a conclusion and list of used literature.

The volume of the bachelor's thesis is 41 pages, it also contains 23 figures, and a list of 25 references.

Содержание

Введение.....	5
1 Анализ существующих решений электронных цифровых подписей	7
1.1 Понятие электронной цифровой подписи	7
1.2 Значение электронной цифровой подписи в современном мире	9
1.3 Технические аспекты создания электронной цифровой подписи	10
1.4 Способы контроля и учета электронных цифровых подписей	14
2 Разработка компьютерной модели системы контроля и учета электронных цифровых подписей в организации.....	18
2.1 Описание функциональных требований к системе	18
2.2 Описание структуры системы.....	21
2.3 Разработка алгоритмов работы системы	23
3 Проектирование интерфейса и разработка приложения.....	28
3.1 Обоснование вида интерфейса	28
3.2 Разработка структуры интерфейса	28
3.3 Руководство пользователя Web-приложения.....	31
3.4 Руководство пользователя приложения для персонального компьютера.	34
Заключение	38
Список используемой литературы	39

Введение

В сегодняшнюю цифровую эпоху электронные подписи стали неотъемлемой частью управления документами в организациях. Электронные подписи обеспечивают безопасный и удобный способ подписания цифровых документов, контрактов и соглашений. По мере расширения использования электронных подписей необходимо отслеживать и учитывать их, чтобы гарантировать их подлинность и целостность. Ручной мониторинг электронных подписей может занимать много времени и быть подверженным ошибкам. Поэтому разработка компьютерной модели системы контроля и учета электронных цифровых подписей в организации может упростить процесс и повысить эффективность. Эта тема диплома направлена на разработку компьютерной модели, которая может управлять и отслеживать электронные подписи в организации, обеспечивая их законность и точность. Предлагаемая модель обеспечит комплексное решение проблем, с которыми организации сталкиваются при управлении электронными подписями, включая проверку, проверку и аудит. Компьютерная модель будет разработана с учетом законодательных и нормативных требований, обеспечивающих безопасность и конфиденциальность электронных подписей. Актуальна данная работа для организаций разных размеров и секторов, включая здравоохранение, финансы и правительство. Предлагаемая компьютерная модель обеспечит безопасный и эффективный способ управления электронными подписями, снижая риск мошенничества, ошибок и несоблюдения требований.

Цель данной бакалаврской работы является, разработать компьютерную модель системы контроля и учета электронных цифровых подписей в организации.

Объектом исследования является система контроля и учета электронных цифровых подписей в организации.

Предметом исследования является разработка компьютерной модели системы контроля и учета электронных цифровых подписей в организации.

Для достижения этой цели необходимо выполнить следующие задачи:

- проанализировать текущее состояние контроля и учета ЭЦП в организации;
- определить ключевые требования и функции, которыми должна обладать предлагаемая система;
- разработать компьютерную модель предлагаемой системы с использованием соответствующих средств программирования;
- оценить производительность и функциональность предлагаемой системы путем тестирования и моделирования.

1 Анализ существующих решений электронных цифровых подписей

1.1 Понятие электронной цифровой подписи

Использование электронных транзакций быстро растет в последние годы. Однако необходимо обеспечить подлинность и целостность электронных документов в цифровом мире. В этом разделе мы обсудим понятие электронной цифровой подписи и ее виды.

Понятие электронной цифровой подписи относится к технологическому решению, позволяющему идентифицировать автора электронного документа или сделки. Этот тип подписи используется для обеспечения подлинности, целостности и неотказуемости электронных данных.

Электронная цифровая подпись – это электронный способ проверки подлинности цифрового документа. Он используется для обеспечения безопасности электронных транзакций, таких как online-банкинг, электронная коммерция и другие формы online-транзакций. Цифровая подпись – это математический алгоритм, который используется для проверки подлинности и целостности цифрового документа [5].

В основном существует два типа электронной цифровой подписи, а именно:

- простая электронная цифровая подпись – это базовая форма электронной подписи, используемая для проверки подлинности цифрового документа. Он используется для подписи содержимого документа и подтверждения личности подписавшего;

- расширенная электронная цифровая подпись обеспечивает более высокий уровень безопасности, чем простая электронная подпись. Он используется для проверки подлинности и целостности цифрового документа. Он также включает дополнительную информацию, такую как отметка времени, свидетельствующая о времени подписания документа. Для этого

требуется использование цифрового сертификата, который выдается доверенным органом.

Электронные цифровые подписи работают с использованием криптографических алгоритмов для создания уникального цифрового отпечатка документа или транзакции. Затем этот отпечаток шифруется с помощью закрытого ключа подписывающей стороны, который можно расшифровать только с помощью его открытого ключа. Таким образом, электронная подпись обеспечивает безопасный способ проверки личности подписавшего и гарантирует, что документ или транзакция не были подделаны [2], [8], [15].

Электронные цифровые подписи юридически признаны во многих странах и часто используются в таких отраслях, как финансы, здравоохранение и правительство. Однако важно отметить, что электронные подписи должны соответствовать определенным юридическим требованиям в каждой юрисдикции, включая использование определенных стандартов и протоколов.

В целом концепция электронной цифровой подписи является важнейшим компонентом цифровой безопасности и обеспечивает надежный способ проверки подлинности и целостности электронных документов и транзакций.

Электронная цифровая подпись необходима по следующим причинам:

- аутентификация: используется для проверки личности подписавшего, что гарантирует, что документ не был подделан;
- целостность: гарантирует, что содержимое документа не было изменено;
- неотказуемость: обеспечивает доказательство того, что подписывающая сторона подписала документ, и подписывающая сторона не может отрицать, что подписала его;
- безопасность: обеспечивает высокий уровень безопасности электронных транзакций, что снижает риск мошенничества.

Электронная цифровая подпись является важнейшим элементом безопасных и безопасных электронных транзакций. Он обеспечивает подлинность, целостность и неотказуемость цифровых документов. Использование электронной цифровой подписи становится все более распространенным по мере того, как мир становится все более цифровым.

1.2 Значение электронной цифровой подписи в современном мире

В сегодняшнюю цифровую эпоху, когда информация передается в электронном виде, потребность в безопасных и надежных средствах аутентификации становится все более важной. Электронные цифровые подписи стали ценным инструментом для достижения этой цели.

Электронная цифровая подпись – это метод проверки подлинности и целостности электронных документов, сообщений или транзакций. Это математический метод, который использует уникальный код или ключ для подписи цифрового документа, и эта подпись затем проверяется получателем с использованием того же ключа. Ценность электронных цифровых подписей заключается в их способности обеспечивать безопасные и удобные средства аутентификации. В отличие от традиционных подписей, электронные подписи нельзя легко подделать или манипулировать. Они также обеспечивают способ аутентификации документов и транзакций без необходимости физического присутствия или бумажной документации.

Электронные цифровые подписи широко используются в современном мире, особенно в сферах электронной коммерции, финансовых транзакций и юридической документации. Они предлагают несколько преимуществ по сравнению с традиционными методами аутентификации, включая более быстрое время обработки, улучшенную безопасность и снижение затрат, связанных с бумажной документацией [12].

Кроме того, электронные цифровые подписи признаны и имеют обязательную юридическую силу во многих странах мира. Это означает, что

их можно использовать для подписания контрактов, соглашений и других юридических документов, обеспечивая уровень безопасности и достоверности, которого трудно достичь с помощью традиционных подписей.

Электронная цифровая подпись (ЭЦП) является важным инструментом аутентификации и обеспечения целостности информации в электронном виде. В современном мире, где электронная коммуникация является неотъемлемой частью бизнеса и повседневной жизни, ЭЦП играет важную роль в обеспечении безопасности электронной переписки и транзакций.

ЭЦП используется во многих отраслях, включая банковское дело, государственную службу, медицину и юриспруденцию, где требуется обеспечить надежность и безопасность передаваемой информации. Благодаря использованию ЭЦП, возможно подтверждение авторства документов, контроль целостности информации и обеспечение подлинности электронных транзакций [9].

Кроме того, использование ЭЦП позволяет ускорить процесс обмена документами и снизить затраты на бумажную документацию и логистику. Это позволяет компаниям повысить эффективность своих бизнес-процессов и улучшить обслуживание своих клиентов [21].

В заключение, значение электронных цифровых подписей в современном мире невозможно переоценить. Они обеспечивают безопасные, надежные и удобные средства аутентификации, которые необходимы в эпоху цифровых технологий. По мере развития технологий электронные цифровые подписи будут играть все более важную роль в обеспечении целостности и подлинности электронных транзакций и документов.

1.3 Технические аспекты создания электронной цифровой подписи

Чтобы создать цифровую подпись, подписывающая сторона должна сначала сгенерировать пару открытого и закрытого ключей. Закрытый ключ держится в секрете подписывающей стороной, а открытый ключ доступен

всем, кто хочет проверить подпись. Затем подписывающая сторона использует закрытый ключ для подписи документа, который создает уникальную цифровую подпись. Цифровая подпись прикрепляется к документу и отправляется получателю вместе с открытым ключом.

Чтобы проверить цифровую подпись, получатель использует открытый ключ для расшифровки подписи и сравнения ее с исходным документом. Если подпись совпадает с документом, то документ не был подделан, а отправитель является тем, за кого себя выдает.

Существует два основных типа цифровых подписей: простые и расширенные. Простая цифровая подпись – это базовая электронная подпись, которая используется для проверки подлинности электронного документа. Усовершенствованная цифровая подпись – это более сложная электронная подпись, отвечающая юридическим требованиям к подписи во многих странах. Для расширенных цифровых подписей требуется сертификат, выданный доверенным центром сертификации, для проверки личности подписавшего [3], [6].

Чтобы обеспечить эффективность цифровых подписей, должны быть выполнены технические требования. Эти требования включают использование безопасного криптографического алгоритма, использование защищенной системы управления ключами и использование безопасного канала связи.

Электронная цифровая подпись создается с помощью алгоритма, который использует открытый и закрытый ключи. Открытый ключ распространяется широко и используется для проверки подписи, а закрытый ключ хранится в секрете и используется для создания подписи.

На рисунке 1 представлена программа подготовки ключей.



Рисунок 1 – Программа подготовки ключей

Создание ЭЦП начинается с хеширования данных, которые должны быть подписаны. Хеш-функция преобразует входные данные в уникальный набор символов фиксированной длины, который называется хешем. Затем закрытый ключ используется для создания подписи, которая представляет собой цифровую метку, привязанную к хешу.

Проверка подписи происходит путем повторного вычисления хеша от исходных данных и сравнения его с полученным хешем из подписи. Затем открытый ключ используется для проверки, что подпись была создана с использованием соответствующего закрытого ключа и что данные не были изменены после создания подписи [14].

Создание и проверка ЭЦП требует вычислительных ресурсов, поэтому существует ряд технических решений, которые облегчают и ускоряют этот процесс. Например, можно использовать аппаратные ускорители для вычисления хеш-функций и создания подписей, а также использовать криптографические протоколы для оптимизации процесса проверки подписи.

На рисунке 2 изображена схема работы цифровой подписи.



Рисунок 2 – Схема работы цифровой подписи

Электронные цифровые подписи являются важным аспектом электронной связи и необходимы для обеспечения подлинности электронных документов. Для создания электронной цифровой подписи используется комбинация криптографических алгоритмов для создания уникальной подписи, которая прикрепляется к документу. Затем подпись проверяется с помощью открытого ключа, чтобы убедиться, что документ не был подделан и что отправитель является тем, за кого себя выдает. Для обеспечения эффективности цифровых подписей должны быть выполнены технические требования, в том числе использование безопасного криптографического алгоритма, защищенной системы управления ключами и защищенного канала связи [10], [13].

1.4 Способы контроля и учета электронных цифровых подписей

Системы контроля и учета электронных цифровых подписей играют важную роль в обеспечении безопасности электронной переписки и транзакций. Они обеспечивают надежную аутентификацию подписавшего и целостность подписываемых данных.

Существует несколько способов контроля и учета электронных цифровых подписей. Рассмотрим их подробнее.

Сертификационный центр (СЦ) – это организация, которая выпускает сертификаты ключей электронной подписи и проверяет подлинность ключей подписи. Сертификат ключа подписи является электронным документом, который содержит информацию о ключе подписи, его владельце и сроке его действия [7].

Сертификационный центр создает удостоверяющий центр (УЦ), который является доверенным лицом, которое проверяет подлинность ключа подписи и выпускает сертификат. УЦ использует цепочку доверия, чтобы проверить, что сертификат был выпущен СЦ [1].

Пользователи могут проверить подлинность ключа подписи, используя сертификат ключа подписи и цепочку доверия. При проверке подписи, пользователь получает сертификат ключа подписи и проверяет его подлинность, затем проверяет цепочку доверия, чтобы убедиться, что СЦ выдал этот сертификат.

Список отозванных сертификатов (СОС) – это список сертификатов, которые больше не могут использоваться для проверки подписи. Сертификаты могут быть отозваны из-за утраты доверия, компрометации ключа подписи или других причин [16].

Сертификационный центр должен поддерживать СОС и регулярно обновлять его. Пользователи должны проверять СОС перед использованием сертификата ключа подписи, чтобы убедиться, что сертификат не был отозван.

Аудит и контроль доступа - это способы контроля и учета электронных цифровых подписей, которые позволяют отслеживать использование ключей подписи и контролировать доступ к ним.

Аудит может включать в себя запись действий, связанных с использованием ключей подписи, таких как создание, проверка или отзыв подписи. Это позволяет отслеживать использование ключей подписи и идентифицировать нежелательные действия.

Контроль доступа может включать в себя установку политик безопасности, которые определяют, кто может использовать ключи подписи и как они могут быть использованы [4]. Например, политика безопасности может запрещать использование ключей подписи без предварительного одобрения или требовать двухфакторной аутентификации для доступа к ключу подписи.

На рисунке 3 изображена схема нанесения и проверки ЭЦП.



Рисунок 3 – Нанесение и проверка ЭЦП

Криптографический токен – это устройство, которое хранит ключи подписи и выполняет операции с ними. Криптографические токены обычно имеют защищенное хранилище для ключей подписи и могут выполнять операции с ними без раскрытия ключей [11].

Криптографические токены обеспечивают дополнительный уровень безопасности, поскольку они могут быть физически защищены и использоваться только авторизованными пользователями.

Электронные цифровые подписи используются для проверки подлинности и целостности электронных документов. Для обеспечения безопасности цифровых подписей важно правильно их контролировать и записывать. Вот несколько способов сделать это:

- контроль доступа. Должен быть установлен контроль доступа, чтобы ограничить круг лиц, которые могут создавать или использовать цифровые подписи. Это помогает предотвратить несанкционированное использование цифровых подписей;

- отзыв сертификата. Цифровые сертификаты, используемые в электронных цифровых подписях, могут быть отозваны, если они больше не действительны. Это помогает предотвратить несанкционированное использование цифровых подписей;

- отметка времени. Отметка времени используется для записи времени создания цифровой подписи. Это помогает доказать подлинность подписи и предотвращает подписание документов после их подделки;

- журналы аудита. Необходимо вести журналы аудита для регистрации всех действий, связанных с цифровыми подписями. Это помогает обнаруживать и предотвращать мошеннические действия, связанные с цифровыми подписями;

- шифрование. Шифрование можно использовать для защиты цифровых подписей от несанкционированного доступа. Это помогает предотвратить несанкционированное использование цифровых подписей.

Внедряя эти элементы управления и механизмы записи, организации могут обеспечить безопасность и целостность своих электронных цифровых подписей.

Выводы по разделу 1

Первый раздел ВКР посвящен анализу существующих решений электронных цифровых подписей.

В нем были рассмотрены понятия электронной цифровой подписи, где были рассмотрены электронные цифровые подписи и выявлено, что они являются важнейшим компонентом цифровой безопасности.

Также были рассмотрены способы контроля и учета электронных цифровых подписей, где были расписаны способы контроля и был сделан вывод, что внедряя эти элементы управления и механизмы записи, организации могут обеспечить безопасность и целостность своих электронных цифровых подписей.

2 Разработка компьютерной модели системы контроля и учета электронных цифровых подписей в организации

2.1 Описание функциональных требований к системе

Опишем функциональные требования системы, система должна:

- обеспечивать возможность создания и хранения ключей подписи для каждого пользователя. Ключи должны генерироваться с использованием криптографических алгоритмов, обеспечивающих высокий уровень безопасности;
- предоставлять возможность для выбора типа ключа подписи (RSA или ECDSA) и длины ключа. Пользователи должны иметь возможность сохранять свои ключи в защищенном хранилище, например, на криптографическом токене или в зашифрованном файле;
- обеспечивать возможность создания электронных цифровых подписей для документов и файлов. Пользователи должны иметь возможность выбирать тип подписи (RSA или ECDSA) и используемый ключ подписи;
- создавать подписи должно происходить путем вычисления хеша от исходных данных и создания подписи с использованием выбранного ключа подписи. Система должна также обеспечивать возможность проверки подписи, включая проверку целостности данных и подлинности ключа подписи;
- обеспечивать возможность учета и контроля доступа к ключам подписи. Пользователи должны иметь возможность просматривать свои ключи и управлять правами доступа к ним;
- обеспечивать возможность аудита действий, связанных с использованием ключей подписи, таких как создание и проверка подписей. Аудит должен включать в себя запись даты, времени и пользователя, выполнившего действие, а также описание действия;

- обеспечивать возможность интеграции с сертификационными центрами (СЦ), чтобы проверять подлинность ключей подписи и выпускать сертификаты ключей подписи. Пользователи должны иметь возможность проверять подлинность сертификатов ключей подписи, используя цепочку доверия, полученную от СЦ;

- обеспечивать возможность управления списками отозванных сертификатов (СОС), чтобы пользователи могли проверять подлинность сертификатов ключей подписи. СОС должен обновляться регулярно и содержать информацию о сертификатах, которые больше не могут использоваться для проверки подписи;

- иметь интуитивно понятный интерфейс пользователя, который позволяет пользователям легко создавать и проверять подписи, управлять своими ключами подписи и просматривать информацию о сертификатах ключей подписи;

- обеспечивать высокую производительность при создании и проверке электронных цифровых подписей, а также учете и контроле доступа к ключам подписи. Время выполнения операций должно быть минимальным, чтобы пользователи могли быстро и эффективно работать с системой;

- обеспечивать высокий уровень безопасности, чтобы защитить ключи подписи и данные, которые подписываются. Система должна использовать криптографические алгоритмы, обеспечивающие высокую стойкость к взлому.

Ключи подписи должны храниться в защищенном хранилище, например, на криптографическом токене или в зашифрованном файле.

Аутентификация и авторизация. Система должна аутентифицировать и авторизовать пользователей, прежде чем разрешить им выполнять какие-либо операции, связанные с электронными цифровыми подписями. Механизм проверки подлинности должен основываться на надежных и безопасных методах проверки подлинности, таких как двухфакторная проверка подлинности [24].

Создание и проверка цифровой подписи. В системе должна быть предусмотрена возможность создания цифровых подписей и проверки их подлинности. Цифровые подписи должны соответствовать соответствующим стандартам и правилам.

Управление ключами. Система должна обеспечивать функции управления ключами, такие как генерация, хранение, распространение и отзыв ключей, используемых для создания и проверки цифровых подписей.

Контрольный след. Система должна вести контрольный журнал всех операций, выполненных с цифровыми подписями. Журнал аудита должен включать такую информацию, как личность пользователя, выполнившего операцию, время и дату операции, а также характер операции.

Отчетность. Система должна предоставлять функции отчетности для создания отчетов по ключевым показателям эффективности, таким как количество созданных и проверенных цифровых подписей, количество отозванных ключей и количество неудачных попыток создать или проверить цифровые подписи [25].

Интеграция. Система должна интегрироваться с другими системами, используемыми организацией, такими как системы управления документами, системы электронной почты и системы управления рабочими процессами.

Требования к производительности. Система должна обеспечивать высокую производительность при создании и проверке электронных цифровых подписей, а также учете и контроле доступа к ключам подписи. Время выполнения операций должно быть минимальным, чтобы пользователи могли быстро и эффективно работать с системой.

Требования к безопасности. Система должна обеспечивать высокий уровень безопасности, чтобы защитить ключи подписи и данные, которые подписываются. Система должна использовать криптографические алгоритмы, обеспечивающие высокую стойкость к взлому.

Ключи подписи должны храниться в защищенном хранилище, например, на криптографическом токене или в зашифров.

В заключение компьютерная модель системы контроля и учета электронных цифровых подписей в организации должна соответствовать функциональным требованиям, изложенным в данном разделе. Эти функциональные требования гарантируют, что система является безопасной, надежной и проверяемой.

2.2 Описание структуры системы

Создание и хранение ключей подписи [18], [20]:

- система должна обеспечивать возможность создания и хранения ключей подписи для каждого пользователя. Ключи должны генерироваться с использованием криптографических алгоритмов, обеспечивающих высокий уровень безопасности;

- система должна предоставлять возможность для выбора типа ключа подписи (RSA или ECDSA) и длины ключа. Пользователи должны иметь возможность сохранять свои ключи в защищенном хранилище, например, на криптографическом токене или в зашифрованном файле.

Создание и проверка электронных цифровых подписей:

- система должна обеспечивать возможность создания электронных цифровых подписей для документов и файлов. Пользователи должны иметь возможность выбирать тип подписи (RSA или ECDSA) и используемый ключ подписи;

- создание подписи должно происходить путем вычисления хеша от исходных данных и создания подписи с использованием выбранного ключа подписи. Система должна также обеспечивать возможность проверки подписи, включая проверку целостности данных и подлинности ключа подписи.

Учет и контроль доступа к ключам подписи:

– система должна обеспечивать возможность учета и контроля доступа к ключам подписи. Пользователи должны иметь возможность просматривать свои ключи и управлять правами доступа к ним;

– система должна также обеспечивать возможность аудита действий, связанных с использованием ключей подписи, таких как создание и проверка подписей. Аудит должен включать в себя запись даты, времени и пользователя, выполнившего действие, а также описание действия.

На рисунке 4 представлена структурная схема.

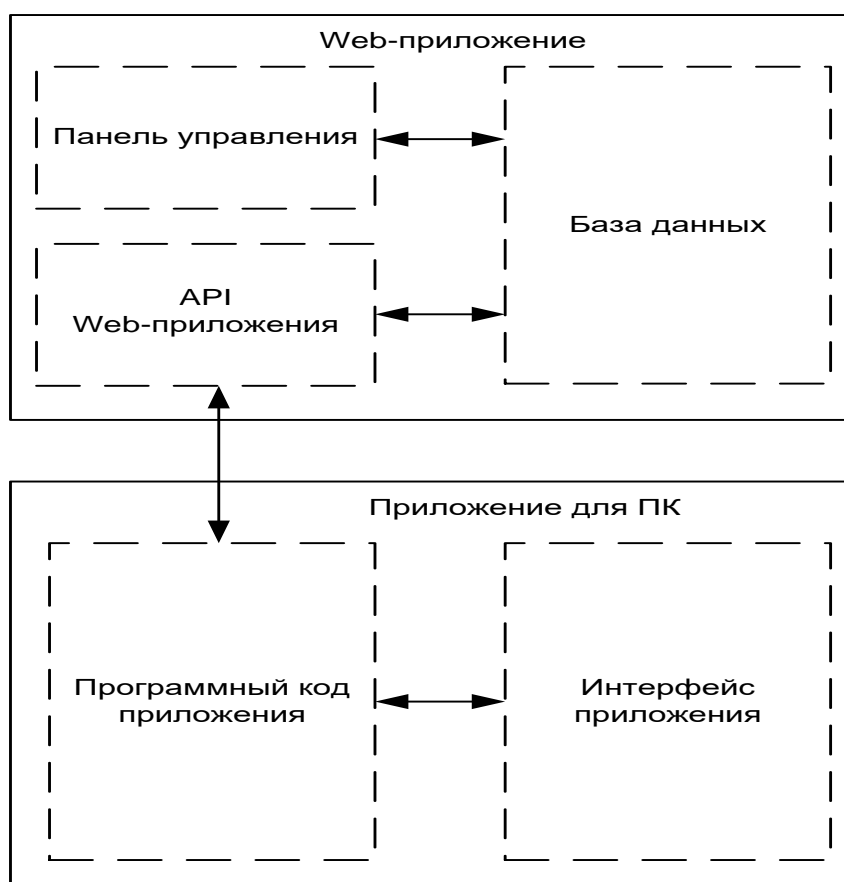


Рисунок 4 – Структурная схема

Интеграция с сертификационными центрами:

– система должна обеспечивать возможность интеграции с сертификационными центрами (СЦ), чтобы проверять подлинность ключей подписи и выпускать сертификаты ключей подписи. Пользователи должны

иметь возможность проверять подлинность сертификатов ключей подписи, используя цепочку доверия, полученную от СЦ.

Управление списками отозванных сертификатов:

- система должна обеспечивать возможность управления списками отозванных сертификатов (СОС), чтобы пользователи могли проверять подлинность сертификатов ключей подписи. СОС должен обновляться регулярно и содержать информацию о сертификатах, которые больше не могут использоваться для проверки подписи.

Интерфейс пользователя:

- система должна иметь интуитивно понятный интерфейс пользователя, который позволяет пользователям легко создавать и проверять подписи, управлять своими ключами подписи и просматривать информацию о сертификатах ключей подписи.

2.3 Разработка алгоритмов работы системы

В этом разделе будут описаны основные шаги, которые пользователи должны выполнить для создания и проверки подписей, управления своими ключами и проверки подлинности сертификатов.

Создание ключей подписи. Алгоритм создания ключей подписи в системе включает следующие шаги [23]:

- пользователь выбирает тип ключа подписи (RSA или ECDSA) и длину ключа;
- система генерирует ключ подписи с использованием выбранных параметров;
- система предоставляет пользователю возможность сохранить ключ на криптографическом токене или в зашифрованном файле.

На рисунке 5 изображена диаграмма компонентов.

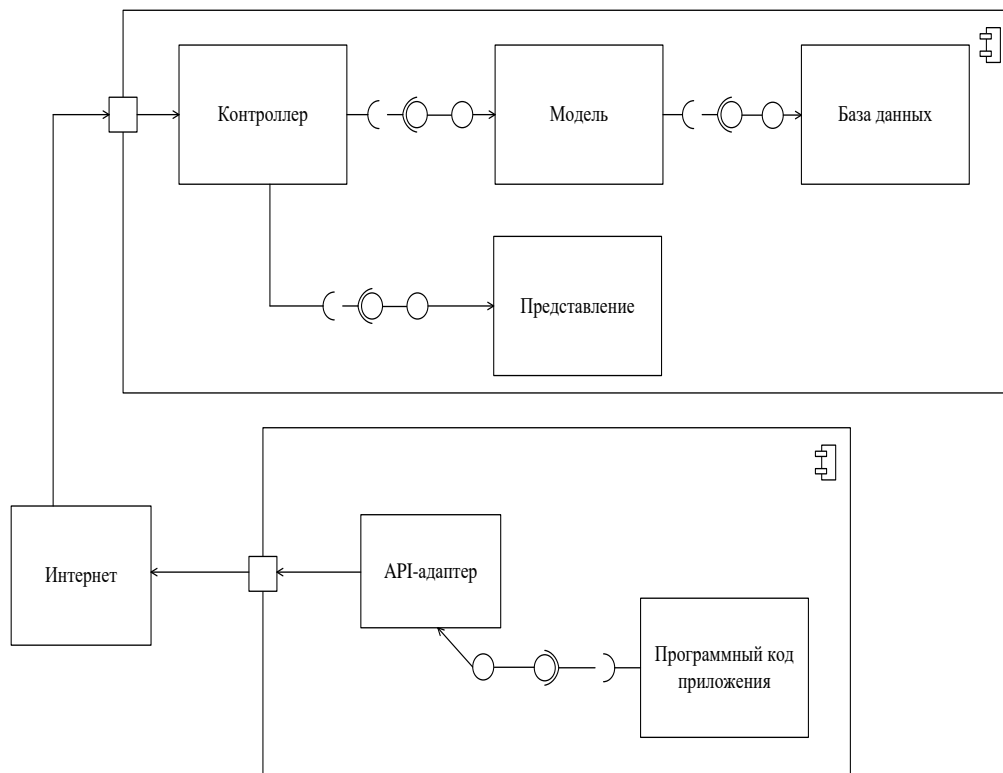


Рисунок 5 – Диаграмма компонентов

Алгоритм создания и проверки подписей в системе включает следующие шаги:

- пользователь выбирает файл для подписи;
- система вычисляет хеш-значение файла;
- пользователь выбирает ключ подписи, используемый для создания подписи;
- система создает подпись с использованием выбранного ключа подписи и хеш-значения файла;
- пользователь может проверить подпись, выбрав файл и подпись, а затем выбрав сертификат ключа подписи;
- система проверяет подпись, используя выбранный сертификат ключа подписи и хеш-значение файла [17].

Блок-схема данного алгоритма представлена на рисунке 6.

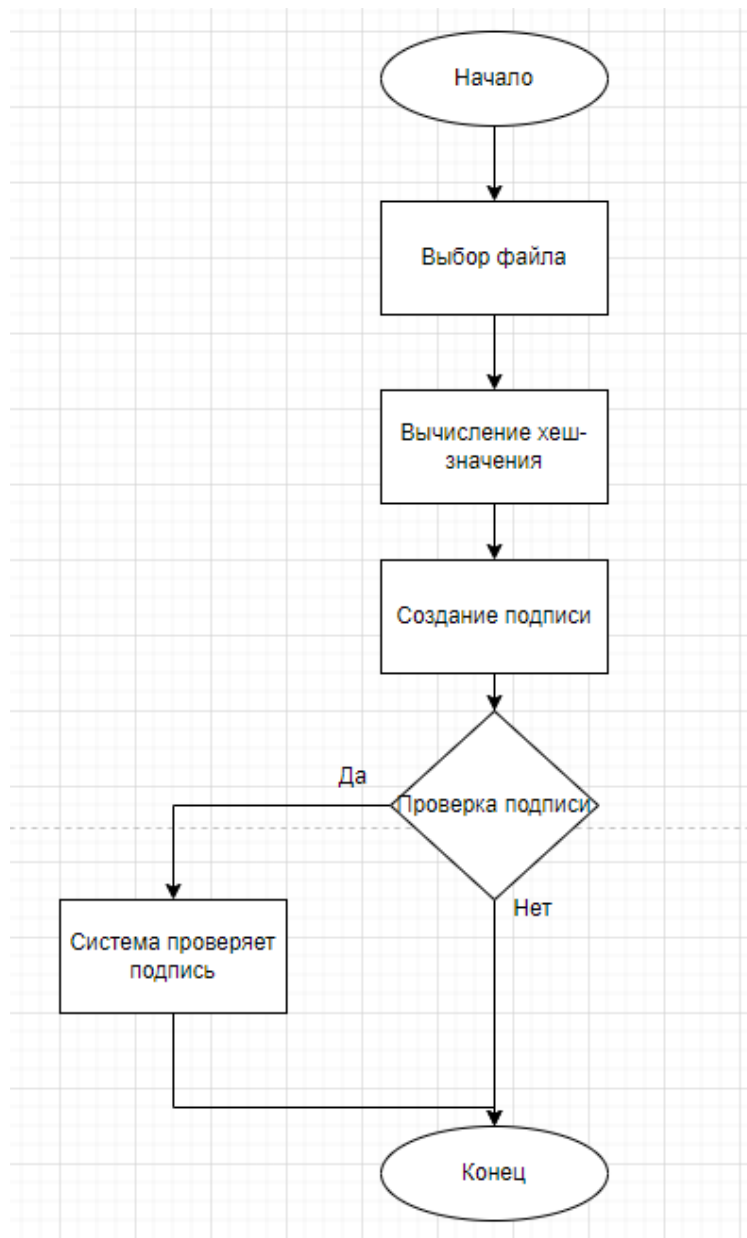


Рисунок 6 – Блок-схема алгоритма создания и проверки подписей в системе

Алгоритм управления ключами подписи в системе включает следующие шаги [19]:

- пользователь выбирает ключ подписи, который он хочет управлять;
- система предоставляет пользователю возможность изменить права доступа к ключу, просмотреть информацию о ключе и удалить ключ.

Блок-схема данного алгоритма представлена на рисунке 7.

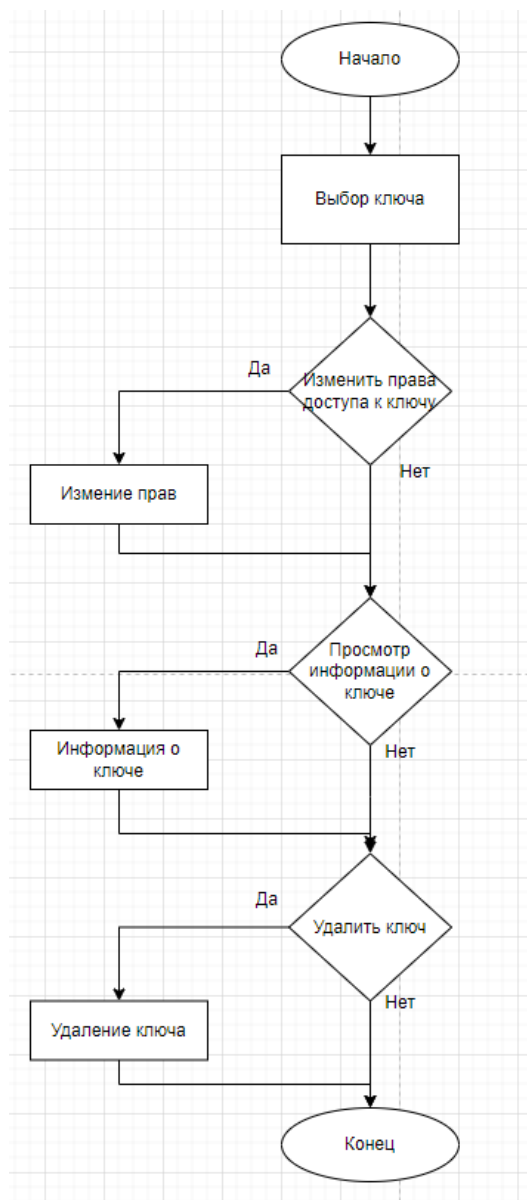


Рисунок 7 – Блок-схема алгоритма управления ключами подписи в системе

Алгоритм проверки подлинности сертификатов ключей подписи в системе включает следующие шаги:

- пользователь выбирает сертификат ключа подписи, который он хочет проверить;
- система использует цепочку доверия, полученную от сертификационного центра, для проверки подлинности сертификата;
- если сертификат действителен, система отображает информацию о сертификате и ключе подписи, связанном с сертификатом.

Блок-схема данного алгоритма представлена на рисунке 8.

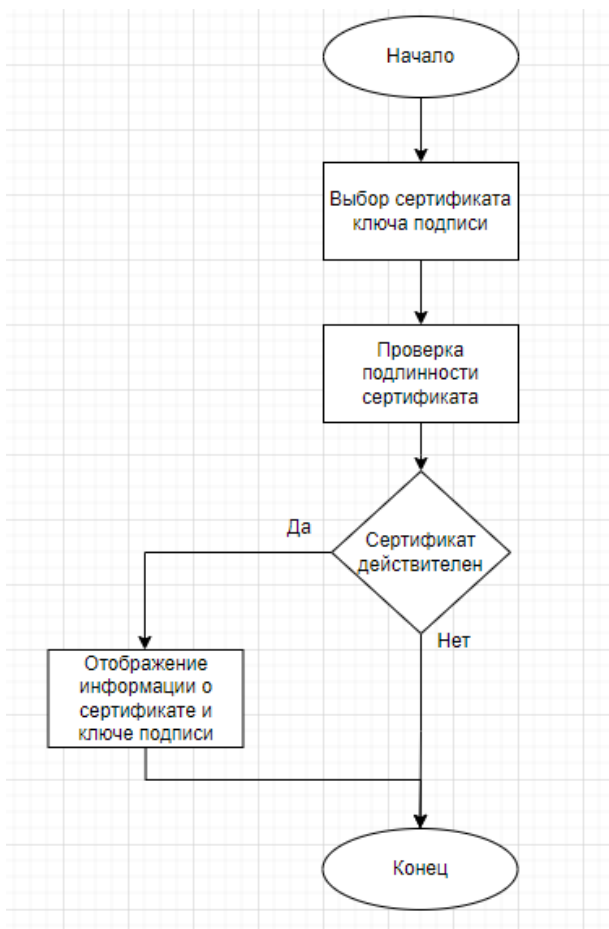


Рисунок 8 – Блок-схема алгоритма проверки подлинности сертификатов ключей подписи в системе

Выводы по разделу 2

Во втором разделе была разработка компьютерной модели системы контроля и учета электронных цифровых подписей в организации.

Были описаны функциональные требования к системе, описана и разработана структурная схема системы и разработка алгоритмов работы системы. После этого можно приступать к проектированию интерфейса и разработке приложения.

3 Проектирование интерфейса и разработка приложения

3.1 Обоснование вида интерфейса

Функциональность приложения – не единственный определяющий фактор его успеха; интерфейс и удобство для пользователя играют не менее важную роль. Многие программы с необходимыми функциями не смогли выйти на рынок из-за неудобных интерфейсов [22].

Чтобы сделать приложение доступным для всех пользователей, крайне важно иметь низкий порог входа и не предполагать высокий уровень компьютерной грамотности.

При разработке приложения с Web-компонентами и ПК-компонентами необходимы отдельные проекты интерфейсов из-за принципиально разных способов реализации интерфейсов.

Интерфейс приложения для ПК создается путем размещения элементов управления на форме во время разработки, а интерфейс Web-API создается с использованием языка разметки HTML в любом текстовом редакторе. Дизайн интерфейса достигается построением макетов в векторном графическом редакторе.

3.2 Разработка структуры интерфейса

Макет страницы авторизации, представленный на рисунке 9.

Он содержит два текстовых поля для ввода имени и пароля пользователя и кнопку подтверждения входа в систему и выхода из системы.

Ввод авторизационных данных

Имя пользователя

Пароль

Войти

Выход

Рисунок 9 – Окно авторизации

При успешной авторизации будет произведен вход в личный кабинет. На рисунке 10 представлено окно личного кабинета пользователя, которое дает возможность просмотреть информацию о сертификатах, подписанных документах и проверить подписи для каждого пользователя, вошедшего в систему.

Личный кабинет

Сертификаты

Подписанные документы

Проверка подписи

Рисунок 10 – Окно личного кабинета пользователя

На рисунке 11 представлена форма, которая отображает информацию. На форме находятся кнопки добавления, удаления сертификата и

формирования заявки на выдачу сертификата. Так же на форме находится поле, в котором выводится информация об имеющихся сертификатах.

Сертификаты

Добавить сертификат Удалить сертификат Заявка на сертификат

Заголовок сертификата 1
Заголовок сертификата 2
Заголовок сертификата 3
Заголовок сертификата 4
Заголовок сертификата 5
Заголовок сертификата 6
Заголовок сертификата 7
Заголовок сертификата 8
Заголовок сертификата 9
Заголовок сертификата 10
Заголовок сертификата 11
Заголовок сертификата 12

Рисунок 11 – Окно списка сертификатов

Рисунок 12 отображает форму «Заявка на сертификат». Для формирования заявки необходима следующая информация: наименование подразделения и должность сотрудника, номер комнаты, где установлено автоматизированное рабочее место, адрес электронной почты, номер телефона, область применения сертификата ключа подписи.

Заявка на сертификат

Наименование подразделения и должность

Номер комнаты, где установлен АРМ

Адрес электронной почты

Номер телефона

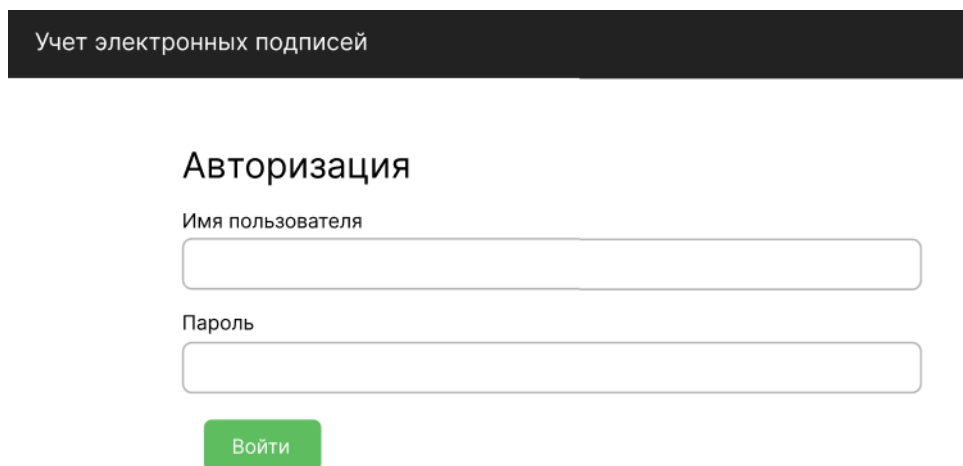
Область применения сертификата ключа подписи

Сформировать заявку Отмена

Рисунок 12 – Окно создания заявки на сертификат

3.3 Руководство пользователя Web-приложения

На рисунке 13 представлено окно авторизации на главной странице, где используются имя пользователя и пароль, которые вводятся в соответствующие поля для заполнения.



Учет электронных подписей

Авторизация

Имя пользователя

Пароль

Войти

Рисунок 13 – Страница «Авторизация»

Именем пользователя является последовательность букв латинского алфавита без специальных символов, длиной не более N символов. Пароль - не превышает 8 символов и состоит из цифр и букв латинского алфавита.

После успешной авторизации пользователь попадает на страницу выбора вменяемых ему функций, например: «Пользователи», «Удостоверяющие центры», «История действий» и «Выход». При выборе интересующей функции открывается окно, где непосредственно создается или редактируется информация.

Для создания нового пользователя необходимо нажать на кнопку «Добавить пользователя», после чего открывается окно, где уже вносятся все необходимые данные, которые нужно опубликовать. Внесенную ранее информацию о пользователе можно отредактировать с помощью кнопки

«Редактировать» или удалить с помощью кнопки «Удалить», как представлено на рисунке 14.

Учет электронных подписей

Пользователь Удостоверяющие центры История действий Выход

Пользователи

→ Добавить пользователя

ID	Имя пользователя	Пользователи	
9	Mgjor gjdk	Администратор	Редактировать Удалить
12	Vladislav Golyb	Сидоров Ян	Редактировать Удалить
13	Ghomehm	Пирогов Петр	Редактировать Удалить
14	Lhjfhttr	Котов Степан	Редактировать Удалить
15	Jremdssfrgth	Фрось Игорь	Редактировать Удалить

Рисунок 14 – Страница «Пользователи»

На рисунке 15 представлена форма «Редактирование пользователя».

Учет электронных подписей

Пользователь Удостоверяющие центры История действий Выход

Редактирование профиля

Имя пользователя

Пароль

Повторите пароль

Полное Имя

[Сохранить](#)

Рисунок 15 – Страница «Редактирование пользователя»

Так же можно добавить новый удостоверяющий центр с помощью кнопки «Добавить удостоверяющий центр». Внесенную ранее информацию об удостоверяющем центре так же можно отредактировать с помощью кнопки «Редактировать» или удалить с помощью кнопки «Удалить», как представлено на рисунке 16.

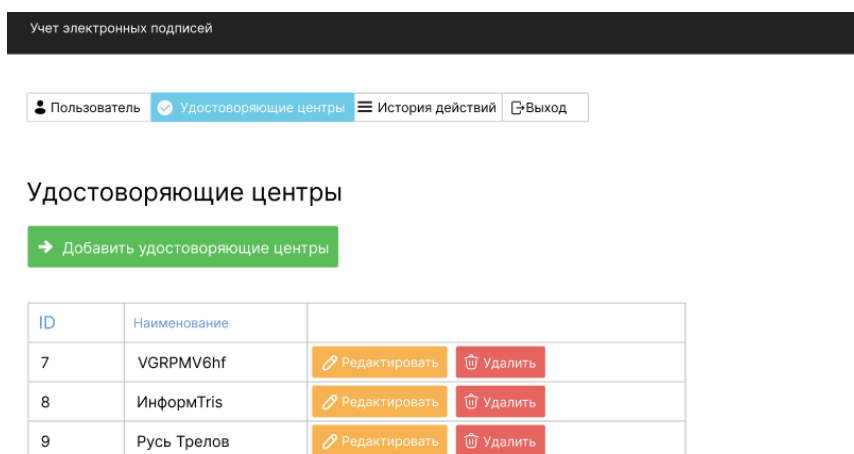


Рисунок 16 – Страница «Удостоверяющие центры»

На рисунке 17 представлено окно, где уже вносятся все необходимые данные, которые нужно опубликовать.

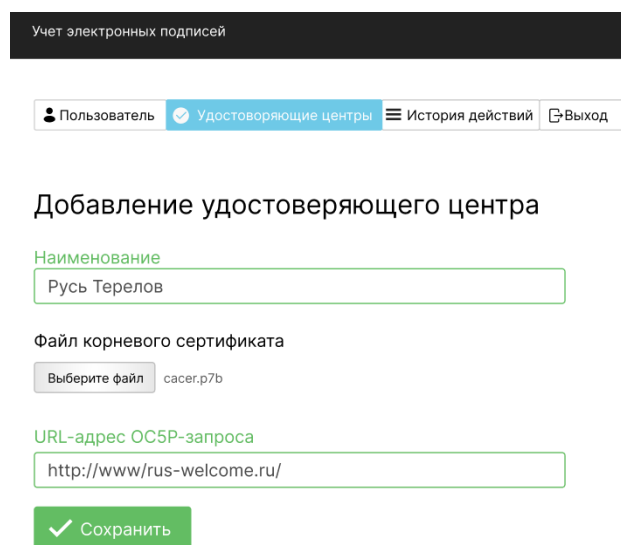


Рисунок 17 – Страница «Редактирование удостоверяющего центра»

На рисунке 18 изображена закладка «История действий» представляет собой журнал истории действий пользователей в системе. Данная информация используется для составления отчетов и ведения учета электронных подписей. С помощью кнопки «Очистить историю» можно удалить весь журнал, или с помощью кнопки «Удалить» удалить некоторые действия совершенные в системе.

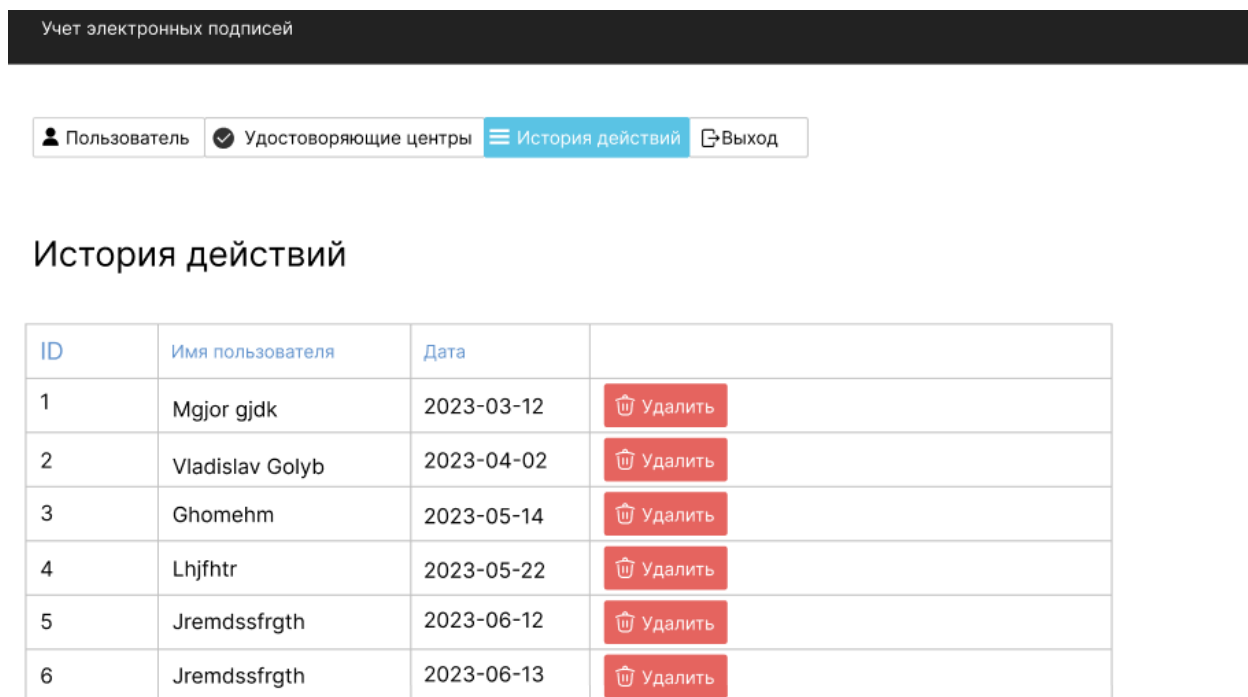


Рисунок 18 – Страница «История действий»

3.4 Руководство пользователя приложения для персонального компьютера

Как представлено на рисунке 19 в приложении для ПК так же присутствует окно авторизации на главной странице, в котором используются имя пользователя и пароль, которые вводятся в соответствующие поля для заполнения.

Именем пользователя является последовательность букв латинского алфавита без специальных символов, длиной не более N символов. Пароль - не превышает 8 символов и состоит из цифр и букв латинского алфавита.

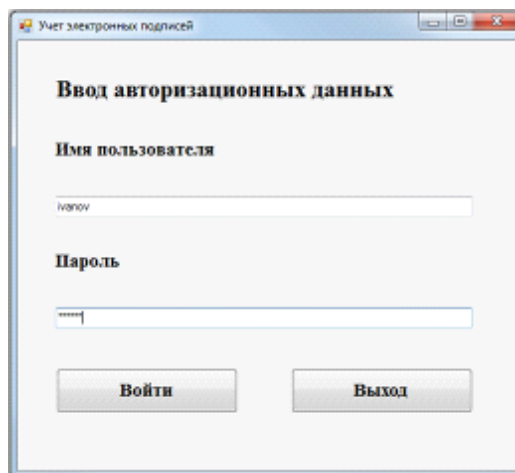


Рисунок 19 – Окно авторизации

После успешной авторизации пользователь попадает в личный кабинет, с кнопками: «Сертификаты», «Подписанные документы» и «Проверка подписи» как представлено на рисунке 20.

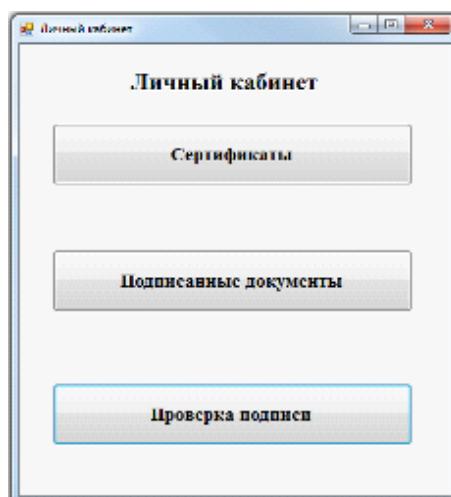


Рисунок 20 – Окно личного кабинета

На рисунке 21 представлен раздел «Сертификаты», где имеется возможность добавить, удалить сертификат и сформировать заявку на сертификат в удостоверяющий центр РЖД. Так же на форме находится поле, в котором выводится информация об уже имеющихся сертификатах.

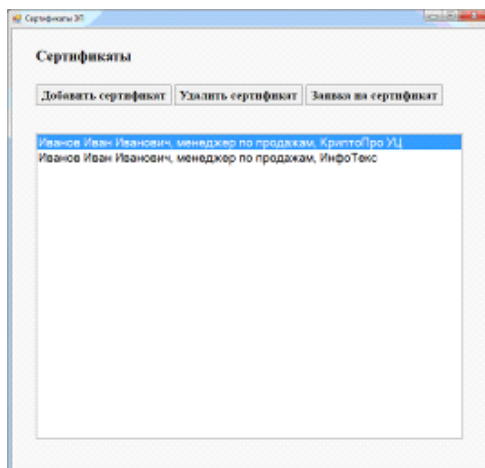


Рисунок 21 – Окно списка сертификатов

На рисунке 22 представлено окно для формирования заявки на сертификат необходимо ввести в поле следующую информацию: наименование подразделения и должность сотрудника, номер комнаты, где установлено автоматизированное рабочее место, адрес электронной почты, номер телефона, область применения сертификата ключа подписи.

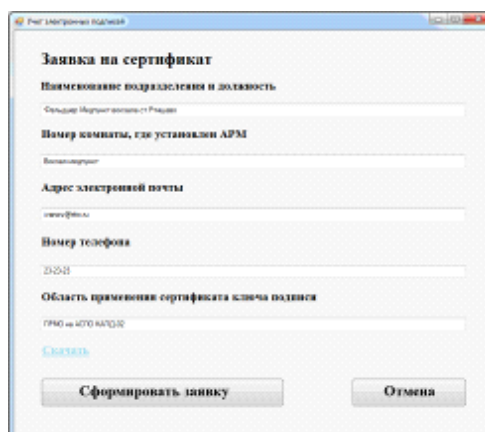


Рисунок 22 – Окно создания заявки на сертификат

С помощью кнопки «Проверка подписи» можно проверить электронную подпись на актуальность, как представлено на рисунке 23.

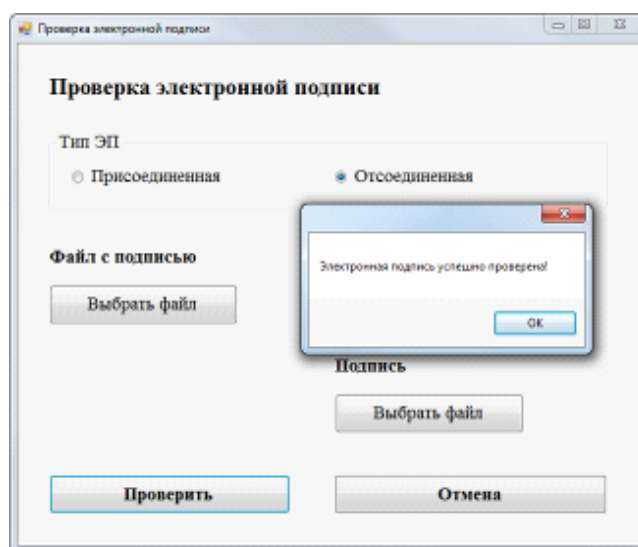


Рисунок 23 – Окно проверки электронной подписи

Выводы по разделу 3

Заключительный раздел ВКР – проектирование интерфейса и разработка приложения.

В этом разделе была разработана структура, после чего приложение было протестировано на разных платформах, а именно Web-приложение и приложение на персональном компьютере. Приложение прошло тестирование, оно работает корректно.

Заключение

Бакалаврская работа посвящена разработке компьютерной модели системы контроля и учета электронных цифровых подписей в организации.

В ходе выполнения ВКР были поставлены задачи на исследования.

Были рассмотрены рассмотрены понятия электронной цифровой подписи, где были рассмотрены электронные цифровые подписи и выявлено, что они являются важнейшим компонентом цифровой безопасности.

Также были рассмотрены способы контроля и учета электронных цифровых подписей, где были расписаны способы контроля и был сделан вывод, что внедряя эти элементы управления и механизмы записи, организации могут обеспечить безопасность и целостность своих электронных цифровых подписей.

Были описаны функциональные требования к системе, описана и разработана структурная схема системы и разработка алгоритмов работы системы.

Была разработана структура, после чего приложение было протестировано на разных платформах, а именно Web-приложение и приложение на персональном компьютере. Приложение прошло тестирование, оно работает корректно.

Задачи, определённые для достижения цели работы, были выполнены в полном объёме, а именно:

- проанализировали текущее состояние контроля и учета ЭЦП в организации;
- определили ключевые требования и функции, которыми должна обладать предлагаемая система;
- разработали компьютерную модель предлагаемой системы с использованием соответствующих средств программирования;
- оценили производительность и функциональность предлагаемой системы путем тестирования и моделирования.

Список используемой литературы

1. Албахари Д. С# 6.0. Справочник. Полное описание языка. 6-е изд. / Албахари Д., Албахари Б. - Москва: OReilly, 2016. - 1040 с.
2. Белло-Орга Н.Н., Огунде А.О. «Обзор систем электронной подписи для управления бизнес-процессами», Международный журнал компьютерных приложений, Vol. 97, № 4, июль 2014 г.
3. Буч Г., Рамбо Д., Якобсон А. Язык UML. Руководство пользователя. Второе издание. ДМК, 2006, 496 с.
4. Виссер Дж. Разработка обслуживаемых программ на языке С# / Виссер Дж. - Москва: ДМК Пресс, 2016. - 292 с.
5. Гольцман В. MySQL 5.0. Библиотека программиста / СПб: Питер, 2010. - 253 с.
6. Гопината С.Д., Балана Р.К. «Структура управления электронными подписями на предприятиях», Журнал управления информационными технологиями, Vol. 17, № 3, 2006.
7. Инюшкина О.Г. Проектирование информационных систем (на примере методов структурного системного анализа): учебное пособие / Екатеринбург: Форт-Диалог Исеть, 2014. - 240 с.
8. Исаев Г.Н. Проектирование информационных систем / Москва: Омега-Л-Москва, 2015. - 512 с.
9. Кумари С.С., Ансари С.А. «Проектирование и внедрение системы управления цифровой подписью для безопасных приложений электронного правительства», Международный журнал передовых исследований в области компьютерных наук и разработки программного обеспечения, Vol. 8, выпуск 11, ноябрь 2018 г.
10. Леоненков А. Самоучитель языка UML. - СПб: БХВ-Петербург, 2007. - 576 с.

11. Оланийи О.О, «Проектирование и внедрение системы управления электронной подписью», Международный журнал компьютерных приложений, Vol. 168, № 13, июнь 2017 г.
12. Опула И.О., АкиниEMI Ф.О. «Проектирование и внедрение системы цифровой подписи для организации», Международный журнал компьютерных наук и мобильных вычислений, Vol. 4, выпуск 4, апрель 2015 г.
13. Рихтер, Дж. CLR via C#. Программирование на платформе Microsoft .NET Framework 4.0 на языке C#. 3-е изд. - СПб.: Питер, 2012. - 982 с.
14. Симдянов И. PHP 7. В подлиннике / Симдянов И., Котеров Д. - Санкт-Петербург: БХВ-Петербург, 2016. - 1073 с.
15. Теслюк Л.М. Оценка эффективности инвестиционного проекта / Теслюк Л.М., Румянцева А.В. - Москва: Фолио, 2011 - 145 с.
16. Шлоснейгл Дж., Профессиональное программирование на PHP / Москва: Вильямс, 2006. - 624 с.
17. Asymmetric cryptography (public key cryptograph). [Электронный ресурс] /Margaret Rouse // SearchSecurity – 05.06.2015 - Режим доступа URL: <https://searchsecurity.techtarget.com/definition/asymmetric-cryptography>
18. Ethereum Yellow Paper [Электронный ресурс] / ethereum.github.io // Dr. Gavin Wood – 28.05.2018 - Режим доступа URL: <https://ethereum.github.io/yellowpaper/paper.pdf>
19. Everything you wanted to know about the next generation of public key crypto.[Электронный ресурс] / Nick Sullivan // Ars Technica – 25.10.2013 – Режим доступа: <https://arstechnica.com/information-technology/2013/10/arelatively-easy-to-understand-primer-on-elliptic-curve-cryptography/2/>
20. RSA algorithm (Rivest-Shamir-Adleman). [Электронный ресурс] /Margaret Rouse // SearchSecurity – 15.05.2014 - Режим доступа URL: <https://searchsecurity.techtarget.com/definition/RSA>

21. Spy-funded privacy tools (like Signal and Tor) are not going to protect us from President Trump [Электронный ресурс] // Yasha Levine / Surveillance Valley – 09.12.2016 - Режим доступа URL: <https://surveillancevalley.com/blog/government-backed-privacy-tools-are-not-going-to-protect-us-from-president-trump>

22. Technology Box — портал посвященный вопросам информационной безопасности. [Электронный ресурс]. - Режим доступа: <http://teh-box.ru/informationsecurity/algorithm-shifrovaniya-rsa-na-palcaх.html>

23. What is Ethereum? [Электронный ресурс] / Alyssa Hertig // CoinDesk – Режим доступа URL: <https://www.coindesk.com/information/what-is-ethereum/>

24. What is symmetric encryption.[Электронный ресурс] / David Bisson // Venafi Blog – 09.11.2017 – Режим доступа: <https://www.venafi.com/blog/whatsymmetric-encryption>

25. White Paper [Электронный ресурс] / GitHub - Режим доступа URL: <https://github.com/ethereum/wiki/wiki/White-Paper>