**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ**

**РОССИЙСКОЙ ФЕДЕРАЦИИ**

**МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ**

**ГЕОДЕЗИИ И КАРТОГРАФИИ (МИИГАиК)**

|  |  |
| --- | --- |
| Факультет: | Геоинформатика и информационная безопасность |
| Направление: | Информационная безопасность |
| Кафедра: | Информационно-измерительных систем |

**ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА**

**на соискание степени бакалавра**

**Тема: «Разработка приложения для анализа криптографических сообщений»**

*СТУДЕНТ:* Сугоняев М.О.

*РУКОВОДИТЕЛЬ:* Матерухин А.В.

*КОНСУЛЬТАНТ:* ( )

*«РАБОТА К ЗАЩИТЕ ДОПУЩЕНА»*

*ЗАВЕДУЮЩИЙ КАФЕДРОЙ* МАЙОРОВ А.А.

МОСКВА 2023 г.

# Содержание

[**Содержание 2**](#_gjdgxs)

**Определения и используемые сокращения 3**

**Введение 4**

**Глава 1 5**

**Заключение 6**

**Список используемых источников 7**

**Приложения 8**

# Используемые сокращения

# Введение

В современном обществе, где цифровые коммуникации играют важнейшую роль, обеспечение безопасности передачи данных становится все более актуальной задачей. Криптография, как наука об обеспечении конфиденциальности, целостности и аутентичности информации, играет важную роль в этом процессе. Одним из ключевых инструментов криптографии является электронная подпись, которая обеспечивает надежность и неподдельность электронных документов и сообщений.

**Актуальность работы** определена совокупностью ряда обстоятельств. В современном информационном обществе электронная подпись стала неотъемлемой частью безопасной передачи данных и обмена информацией [1]. Она играет важную роль в обеспечении целостности, аутентичности и конфиденциальности электронных документов, а также в подтверждении авторства и отказе от возможности отрицания совершенных действий.

Федеральный закон "Об электронной подписи" [2] устанавливает правовые основы использования электронной подписи в Российской Федерации. Закон регулирует вопросы создания, использования и проверки электронной подписи. Однако, существует множество различных спецификаций электронной подписи, которые используются в разных системах и приложениях. Каждая из них может иметь свои особенности, форматы данных и протоколы взаимодействия. В результате возникают сложности при интеграции и взаимодействии между разными системами, что затрудняет обмен электронными документами и проверку электронных подписей.

Согласно статье "Towards a Unified Approach for Interoperability of Electronic Signatures" [3], проблема взаимодействия различных спецификаций электронной подписи заключается в отсутствии единых стандартов и совместимости между различными системами. Авторы указывают, что различные спецификации часто используют разные форматы и протоколы, что затрудняет обмен и проверку электронных подписей между разными системами. Это приводит к необходимости создания дополнительных адаптеров и конвертеров, что увеличивает сложность процесса и снижает эффективность использования электронных подписей, а это несет образование дополнительных издержек при использовании системы электронного документооборота.

Также огромное значение в контексте электронных документов и безопасности информации имеет создание инструмента, который предоставлял бы понятные и ясные объяснения о значениях и атрибутах электронной подписи. Согласно Закону "Об электронной подписи" [1], электронная подпись является важным инструментом для определения лица, подписывающего информацию. Однако, множество атрибутов и значений, связанных с электронной подписью, могут быть сложными для понимания обычными пользователями.

Исследования, проведенные в рамках статьи "Towards a Unified Approach for Interoperability of Electronic Signatures" [2], также подтверждают, что недостаток ясности и понятности объяснений атрибутов электронной подписи является одной из проблем, с которыми сталкиваются пользователи. Недостаточное понимание значений и атрибутов электронной подписи может привести к неправильному использованию или недоверию к этому инструменту, что негативно сказывается на эффективности его применения.

Создание инструмента, который бы предоставлял ясные объяснения о значениях и атрибутах электронной подписи, позволит пользователям лучше осознавать и оценивать все аспекты, связанные с использованием электронной подписи. Он может предоставлять информацию о различных типах электронных подписей, спецификациях, используемых алгоритмах шифрования и ключевых параметрах, а также о технических и юридических требованиях к электронным подписям. Такой инструмент будет полезен как для обычных пользователей, которым требуется простая и понятная информация о значении электронной подписи, так и для специалистов в области информационной безопасности, которые нуждаются в детальной информации о технических деталях и стандартах.

**Целью** данной работы является исследование разработка инструмента, который не только будет проверять корректность электронной подписи различных спецификаций, но и будет предоставлять понятные и ясные объяснения о значениях и атрибутах, связанных с целью упростить понимание и облегчить взаимодействие пользователей с подписанными документами. Создание такого инструмента позволит улучшить процессы проверки электронных подписей и обеспечить дополнительный уровень доверия к электронным документам и сообщениям.

Для реализации цели были решены следующие **задачи**:

1. Описать технологию электронной подписи
2. Изучить существующие стандарты и спецификации электронной подписи для получения глубокого понимания их особенностей, принципов работы и функциональных возможностей.
3. Определить критически важные атрибуты электронной подписи, необходимые для обеспечения безопасности, а также определить менее значимые атрибуты, которые имеют меньшее влияние на безопасность.
4. Изучить существующие решения, выявить их особенности
5. Изучить требования к разрабатываемому алгоритму проверки корректности электронной подписи, включая анализ значений и атрибутов, а также требования к алгоритму предоставления понятных и ясных объяснений о значениях и атрибутах подписи.
6. Разработать алгоритм для определения атрибутов электронной подписи.

**Предмет** **исследования** данной дипломной работы: разработка приложения для анализа атрибутов электронной подписи.

**Объект исследования** данной дипломной работы является электронная подпись и ее атрибуты.

**Нормативную базу** исследования составляет официальная документация стандартов и рекомендаций в области обеспечения информационной безопасности, а также федеральное законодательство, нормативные правовые акты Президента Российской Федерации и Правительства Российской Федерации.

**Научная новизна исследования.**

**Практическая значимость.**

**Структура работы.** Выпускная квалификационная работа состоит из введения, трех глав, заключения, библиографического списка и приложений. Объём работы составляет (ну где-то 60+) страниц печатного текста, в том числе *(много)* приложений на *(много)* страницах. В основном тексте содержатся 1 рисунок и *(много)* таблиц. Список использованных источников и литературы состоит из *(много)* наименований.

В результате работы будет получен ценный инструмент для пользователей, нуждающихся в проверке электронных подписей и анализе содержания подписываемых аргументов. Созданный инструмент способствует повышению доверия к электронным документам и информационным системам, а также способствует обеспечению безопасности и сохранении целостности данных в современном цифровом мире.

# Глава 1. Сведения о предметной области

# Заключение

# Список используемых источников

1. Закон Российской Федерации "Об электронной подписи" от 25 марта 2011 года № 63-ФЗ // Официальный интернет-портал правовой информации. - 2011 г. - с изм. и допол. в ред. от 28.12.2022.

# Приложения