**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

**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.

**Цель данной работы**: 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.

В ходе работы будут рассмотрены основные понятия и принципы, лежащие в основе электронной подписи, их функциональности и ограничений. На основе полученных результатов будет разработан и реализован собственный инструмент, способный эффективно проверять корректность подписи и определять, какие аргументы были подписаны, а какие нет.

Кроме того, проведение тестирования и оценка созданного инструмента позволяет определить его эффективность и применимость в различных сценариях использования. Будут выявлены преимущества и недостатки разработанного решения.

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.

Продолжение работы будет посвящено подробному анализу основных понятий и принципов работы электронной подписи, а также разработке и реализации инструмента для проверки электронной подписи и аргументов.

# 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