

Разработка приложения для формирования цифровой подписи в электронном документообороте

Научный руководитель: Акуленок И. Н.
Исполнитель: Бочкарев В. Д.

Цели работы

- Проанализировать криптографические свойства алгоритмов;
- Реализовать приложение для работы с электронно-цифровой подписью.

Актуальность данной темы – переход крупных производств от бумажного документооборота к электронному, необходимость защищать подлинность таких документов.

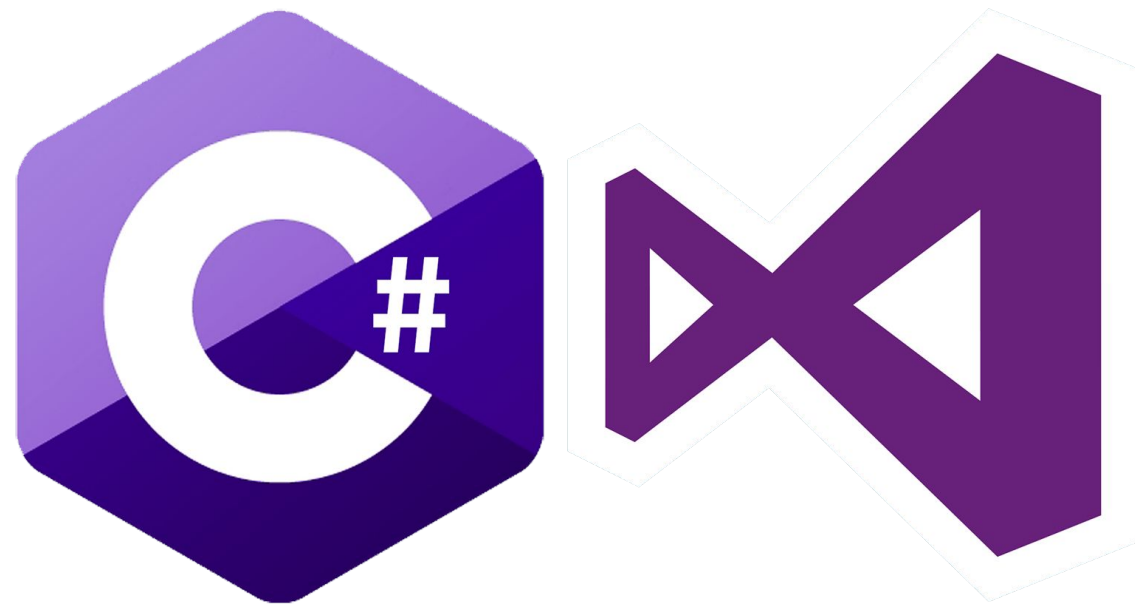
Требования к приложению

Приложение должно выполнять следующие функции:

- Генерировать ключи;
- Формировать подпись и сертификат;
- Проверять корректность подписи и подлинность документа.

Выбор программных средств

- Язык программирования C#
- Платформа .NET Framework версии 7.2.0
- IDE Microsoft Visual Studio 2019
- СУБД SQLite



Предметная область

Документы

Электронные документы

Цифровизация производств

Методы защиты

Основные методы защиты:

1. Загрузка в облачные сервисы
2. Шифрование данных документа
3. Электронно-цифровая подпись

Обзор существующих программ



КриптоАРМ

1. Платное ПО
2. Подпись для разного рода файлов
3. Поддержка стандартов Microsoft CryptoAPI



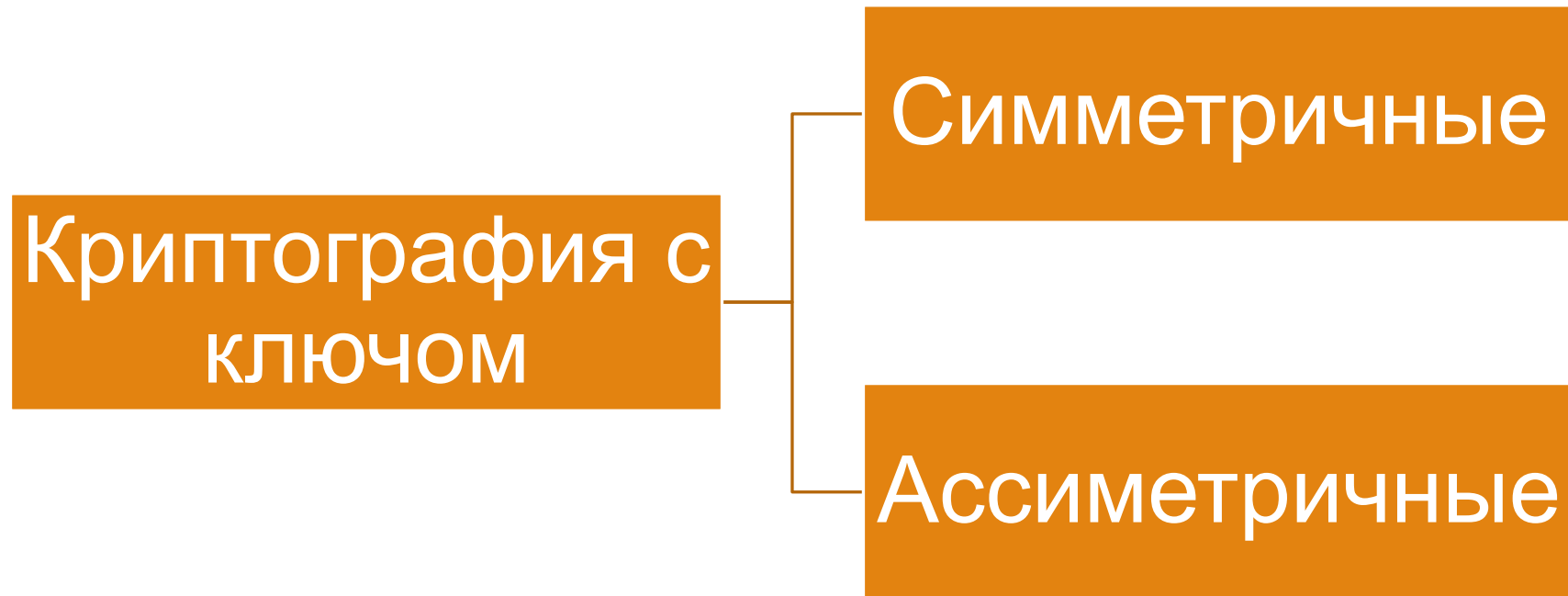
1. Комплексный продукт
2. Поддержка стандартов Microsoft CryptoAPI



SignMachine

1. Бесплатное ПО
2. Необходим сертификат

Виды криптоалгоритмов



Электронно-цифровая подпись

ЭЦП – это цифровая информация, размер которой зависит от алгоритма, которая присоединяется к тексту, и передается уже вместе с ним.

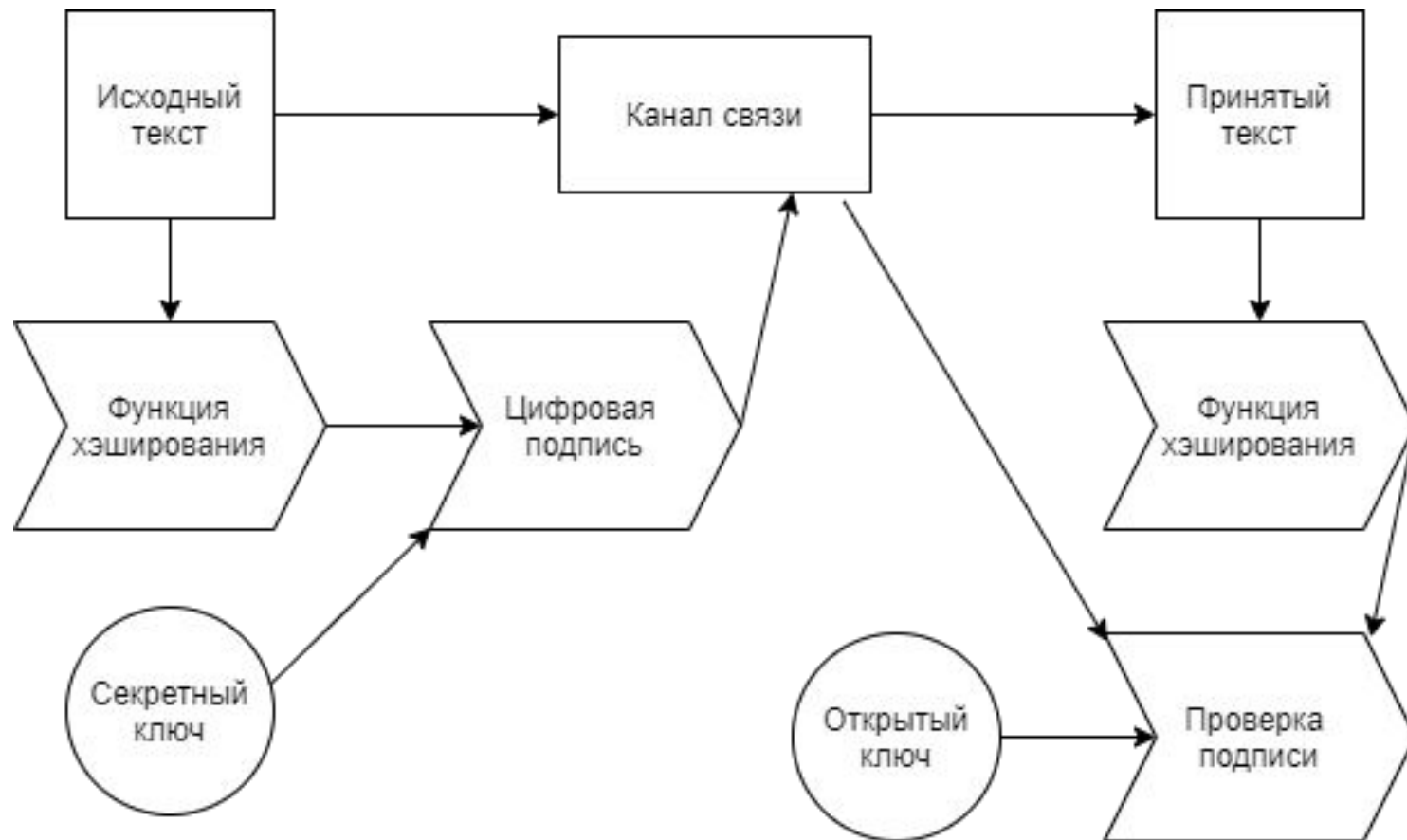
Функции ЭЦП

Удостоверяет
личность
подписавшего
документ

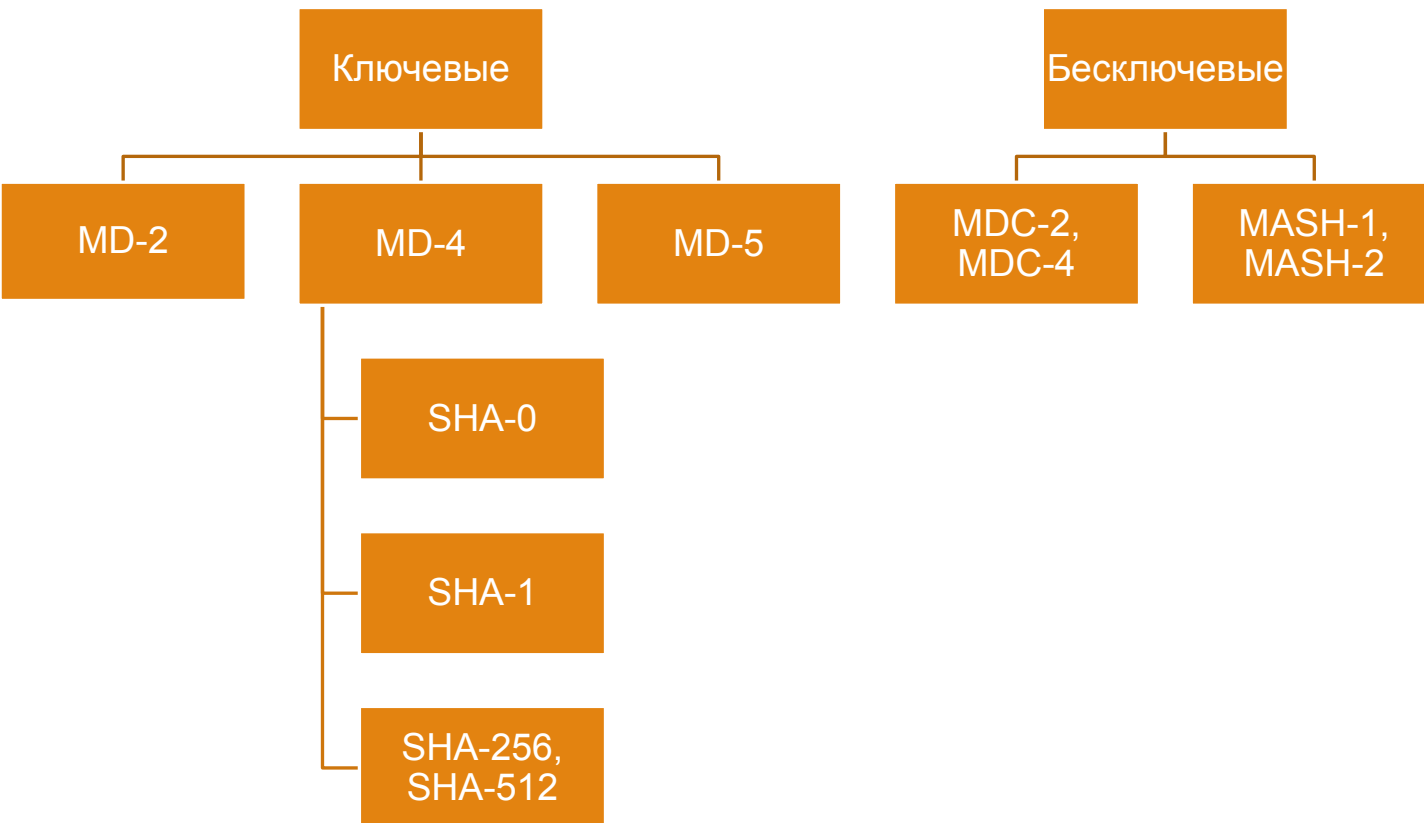
Гарантирует
целостность
документа

Обеспечивает
неотказуемос
ть от
подписанного
документа

Обобщенная схема работы ЭЦП



Функции хэширования



Требования к функциям хэширования:

- Стойкость к поиску первого прообраза
- Стойкость к поиску второго прообраза
- Стойкость к коллизиям

Диаграмма классов

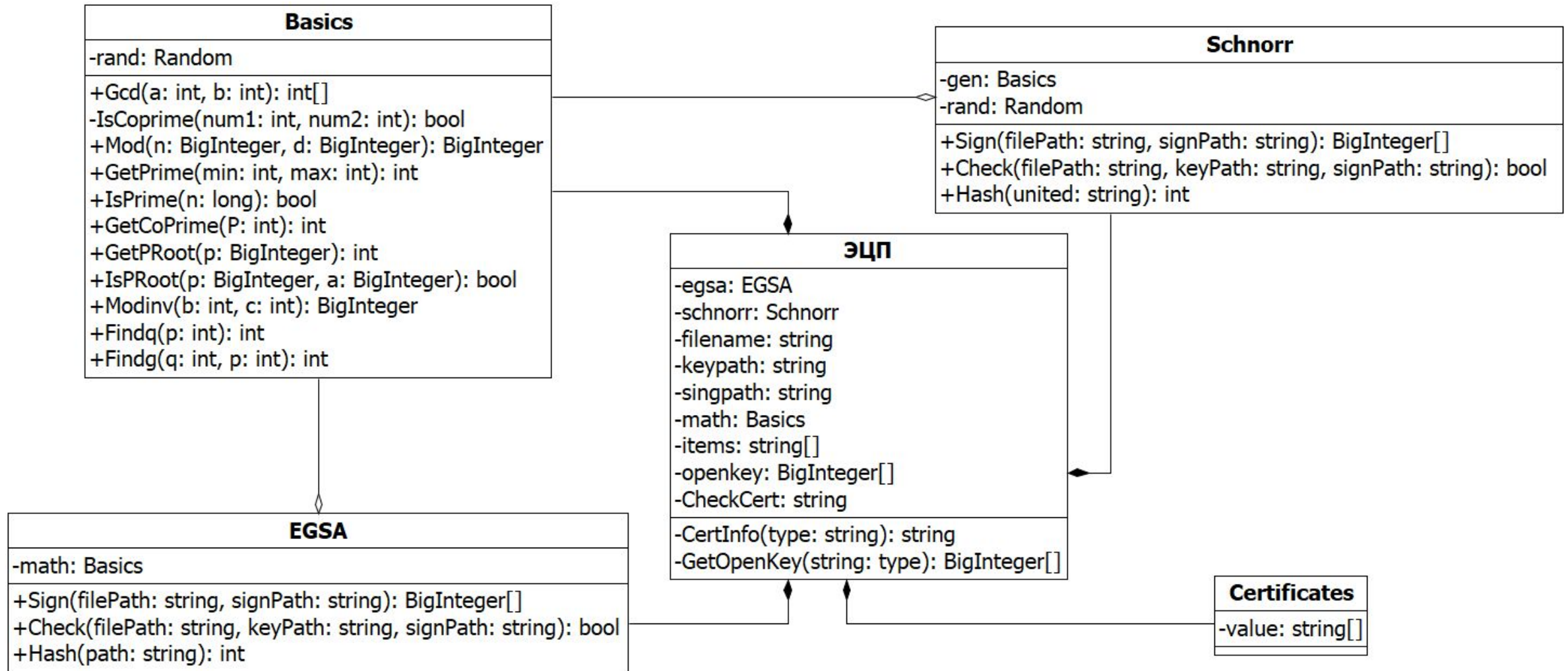
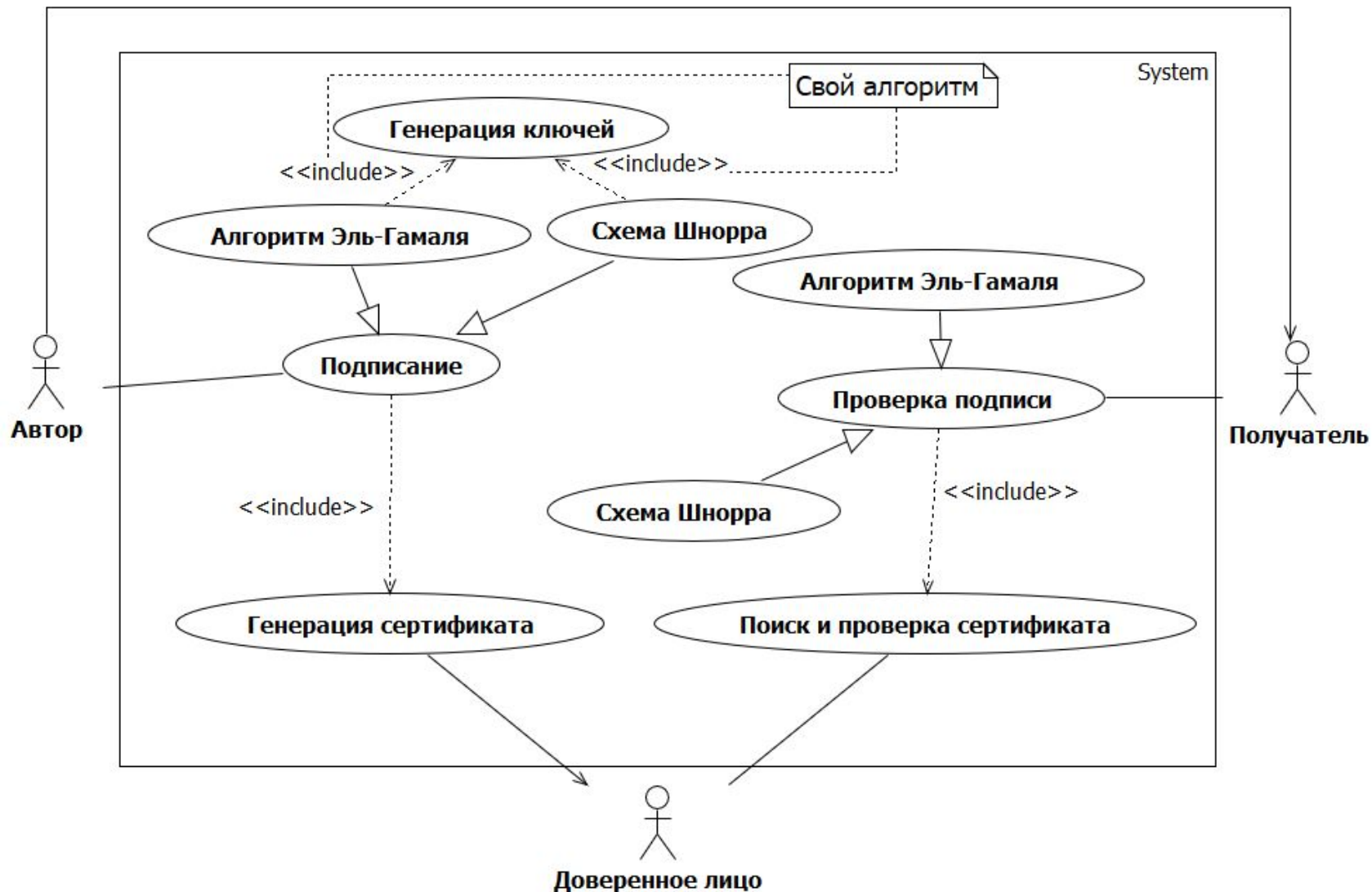


Диаграмма прецедентов



Алгоритм Эль-Гамала

Основные методы разработанного приложения:

- **Sign** реализует основные алгоритмы Эль-Гамала: генерации ключей и формирования подписи;
- **Check** реализует основные алгоритмы проверки подписи;
- **Gcd** реализует расширенный алгоритм Евклида ;
- **Mod** реализует корректное вычисление деления по модулю отрицательных чисел;
- **GetCoPrime** реализует проверку чисел на взаимную простоту;
- **Hash** реализует хэш-функцию SHA-256;
- **IsPRoot** проверяет, является ли число первообразным корнем другого числа.

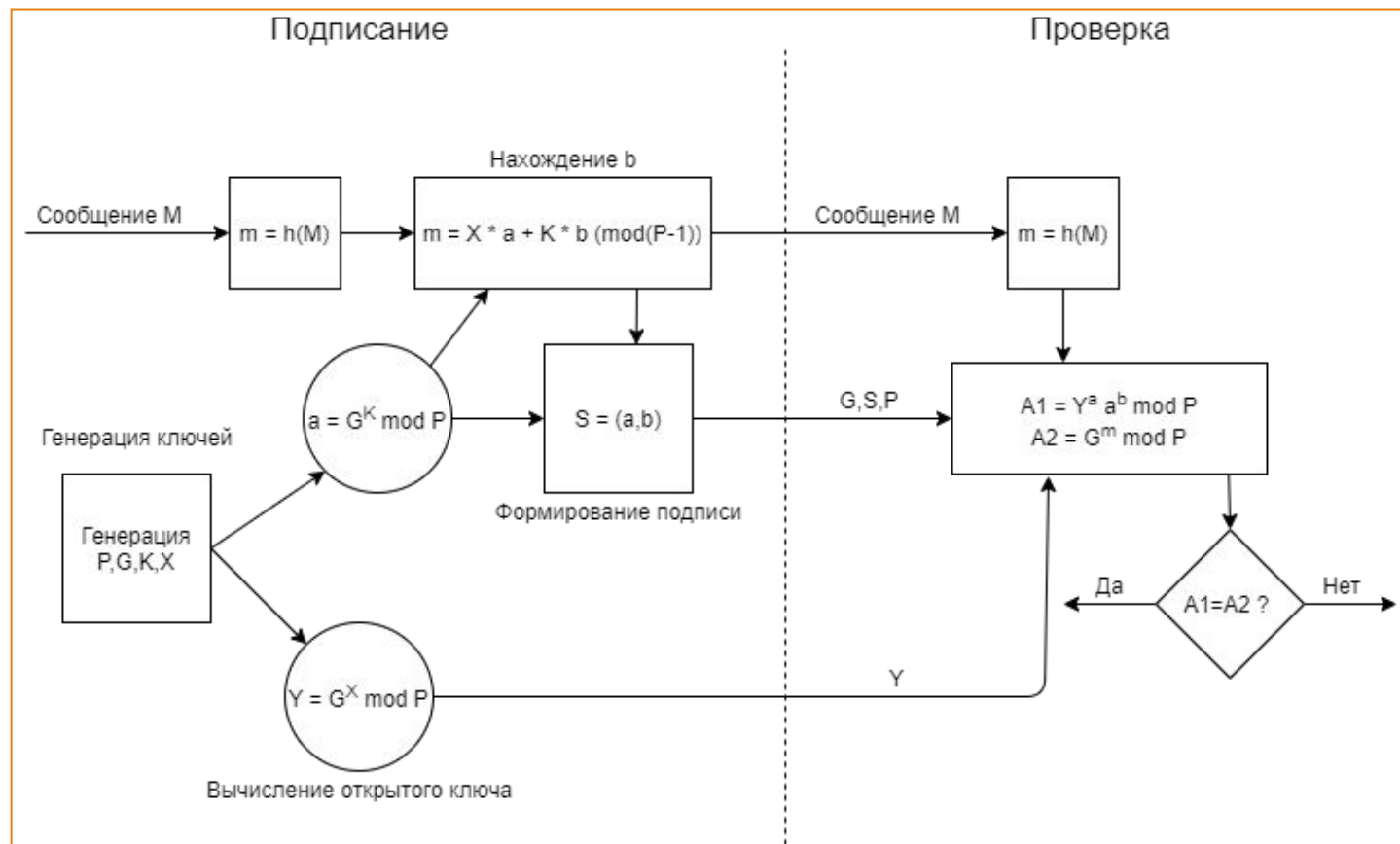
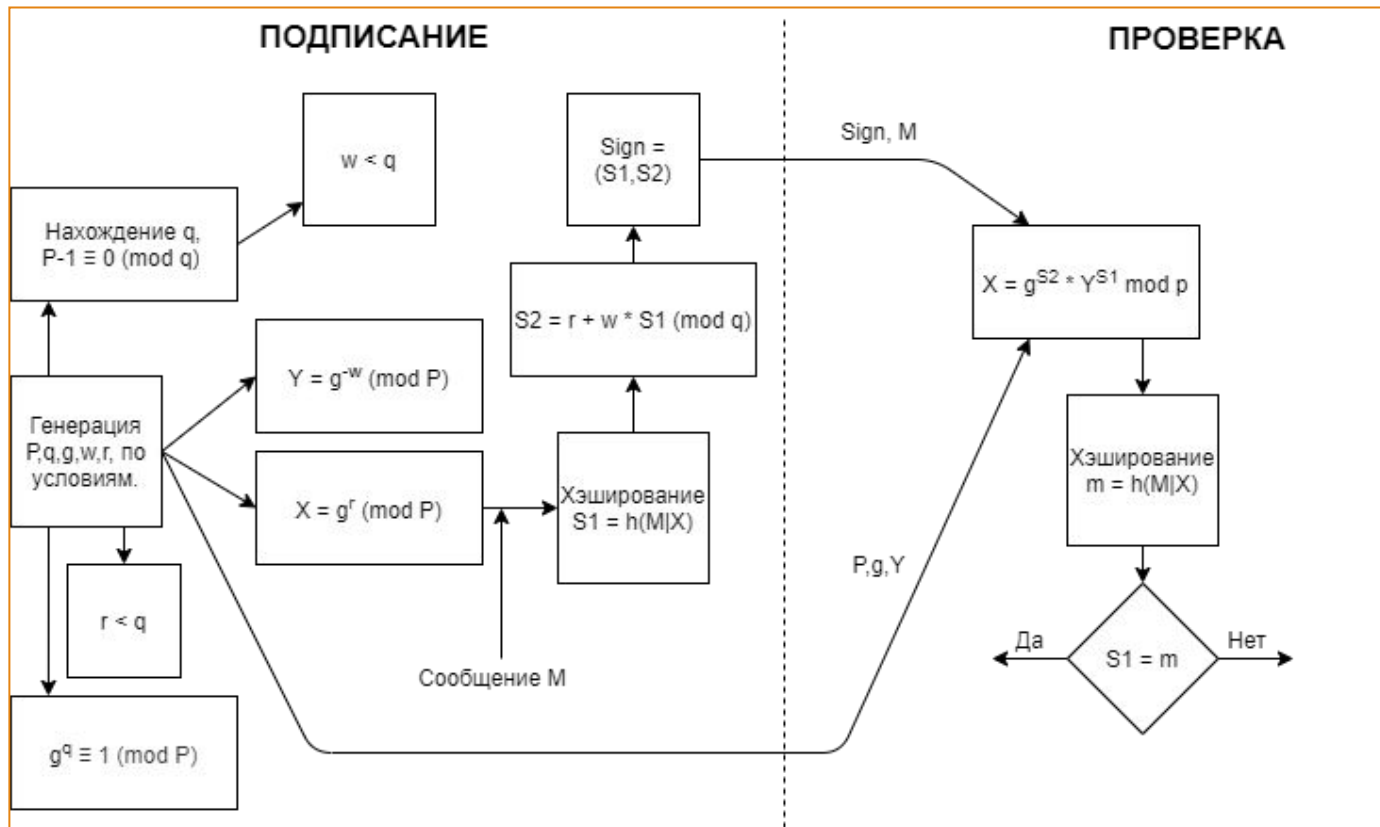


Схема Шнорра



Основные методы разработанного приложения:

- **Sign** реализует основные алгоритмы Шнорра: генерации ключей и формирования подписи;
- **Check** реализует основные алгоритмы проверки подписи;
- **Hash** реализует хэш-функцию MD5;
- **Modinv** реализует нахождение мультипликативного обратного.

Руководство пользователя - подпись

Электронно-цифровая подпись

Окно состояния

Файл подписан

Генерация ключей:
Случайное простое $P = 967$
Случайное простое G меньше $P = 5$
Секретный ключ $X = 569$
Открытый ключ $Y = 883$
Случайное взаимно простое с P число $K = 95$

Подпись:
 $A = 313$
 $B = 916$
ЭЦП = 1001110011110010100
Дайджест для сообщения M : 4297

Работа с документами

Выбор алгоритма ЭЦП
1. ЭЦП Эль-Гамала

Загрузить

Подписать

Проверить

Модуль тестирования

Генерация простого числа

Сгенерировать

Тестирование

Сертификат открытого ключа

Дата начала действия ключа:
12.06.2021 16:22:26
Дата окончания действия ключа:
17.06.2021 16:22:26
Имя подписавшего: Ivan
Фамилия подписавшего: Ivanov
Отчество подписавшего: Ivanovich
Первая часть открытого ключа: 883
Вторая часть открытого ключа: 967
Третья часть открытого ключа: 5
Метод подписи: EGSA
Имя подписанного файла: Документ копия (3).docx

Сертификация

Сертификата открытого ключа ЭЦП

Введите Фамилию
Ivanov

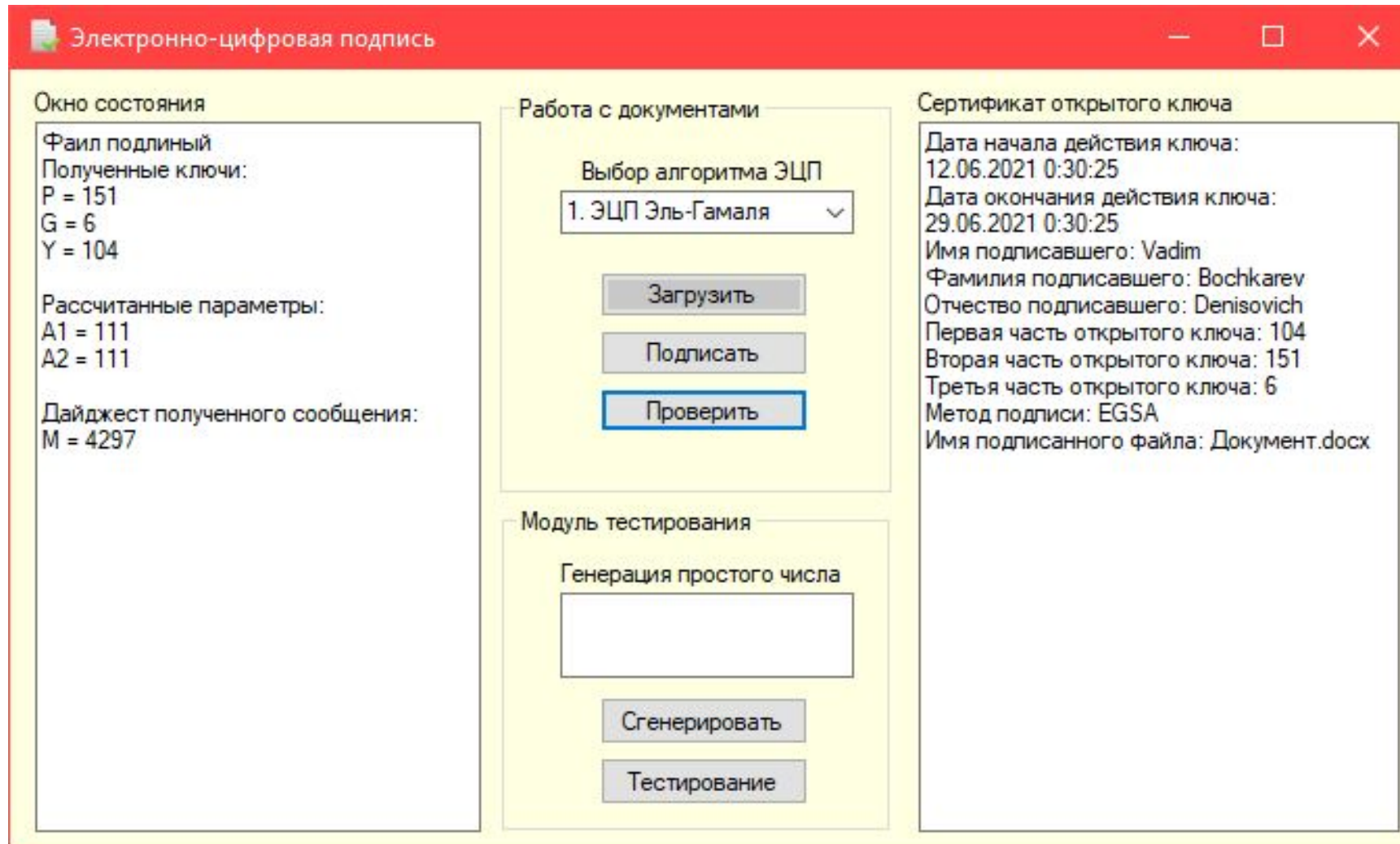
Введите Имя
Ivan

Введите Отчество
Ivanovich

Выберете дату окончания работы сертификата
19 июня 2021 г.

Сертифицировать

Руководство пользователя - проверка



Тестирование и отладка

В данной работе проверялись:

- главная форма приложения и элементы управления;
- операция возведения в степень на переполнение (типа данных BigInteger);
- стандартный оператор модульного деления C# на работу с отрицательными числами;
- корректность выполнения алгоритмов формирования ЭЦП;
- корректность проверки сертификата на принадлежность к документу.

Заключение

- Проанализированы два алгоритма формирования ЭЦП.
- Реализовано приложение для работы с электронно-цифровой подписью.
- Реализованное приложение успешно протестировано.

Спасибо за внимание!