Белорусско-Российский университет
Кафедра «Программное обеспечение информационных технологий»

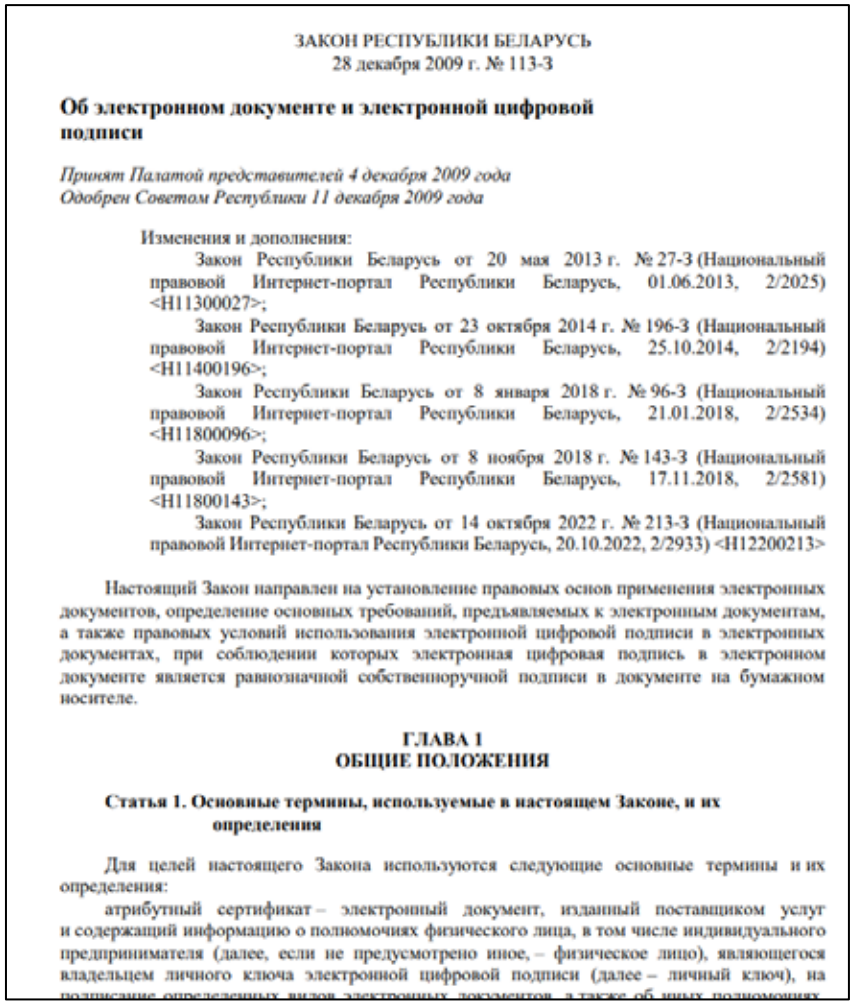
Защита информации

Электронная цифровая подпись

КУТУЗОВ Виктор Владимирович

Республика Беларусь, Могилев, 2024

Закон Республики Беларусь от 28 декабря 2009 г. № 113-З «Об электронном документе и электронной цифровой подписи»



ЗАКОН РЕСПУБЛИКИ БЕЛАРУСЬ
28 декабря 2009 г. № 113-З

Об электронном документе и электронной цифровой подписи

Принят Палатой представителей 4 декабря 2009 года
Одобрен Советом Республики 11 декабря 2009 года

Изменения и дополнения:

Закон Республики Беларусь от 20 мая 2013 г. № 27-З (Национальный правовой Интернет-портал Республики Беларусь, 01.06.2013, 2/2025) <H11300027>;

Закон Республики Беларусь от 23 октября 2014 г. № 196-З (Национальный правовой Интернет-портал Республики Беларусь, 25.10.2014, 2/2194) <H11400196>;

Закон Республики Беларусь от 8 января 2018 г. № 96-З (Национальный правовой Интернет-портал Республики Беларусь, 21.01.2018, 2/2534) <H11800096>;

Закон Республики Беларусь от 8 ноября 2018 г. № 143-З (Национальный правовой Интернет-портал Республики Беларусь, 17.11.2018, 2/2581) <H11800143>;

Закон Республики Беларусь от 14 октября 2022 г. № 213-З (Национальный правовой Интернет-портал Республики Беларусь, 20.10.2022, 2/2933) <H12200213>

Настоящий Закон направлен на установление правовых основ применения электронных документов, определение основных требований, предъявляемых к электронным документам, а также правовых условий использования электронной цифровой подписи в электронных документах, при соблюдении которых электронная цифровая подпись в электронном документе является равнозначной собственноручной подписи в документе на бумажном носителе.

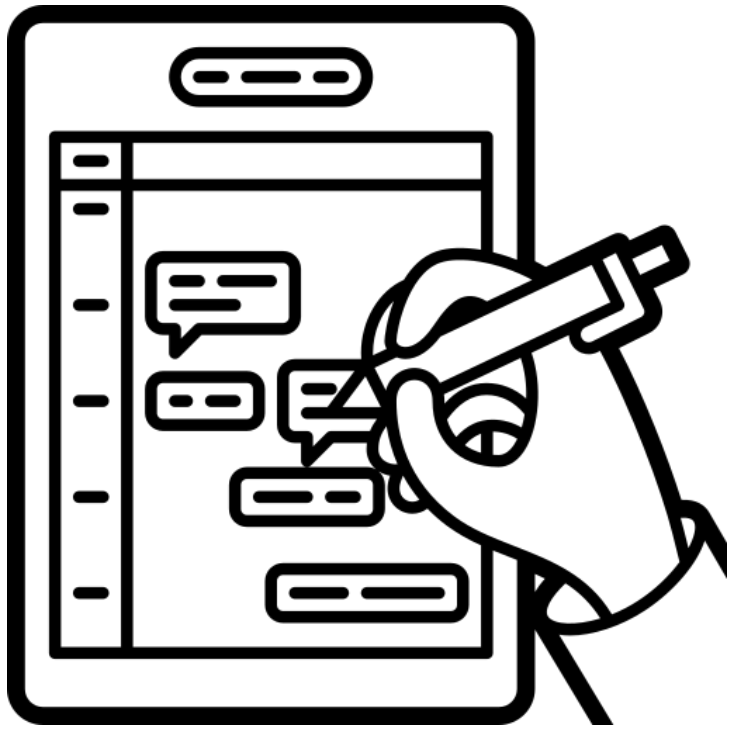
ГЛАВА 1
ОБЩИЕ ПОЛОЖЕНИЯ

Статья 1. Основные термины, используемые в настоящем Законе, и их определения

Для целей настоящего Закона используются следующие основные термины и их определения:

атрибутный сертификат – электронный документ, изданный поставщиком услуг и содержащий информацию о полномочиях физического лица, в том числе индивидуального предпринимателя (далее, если не предусмотрено иное, – физическое лицо), являющегося владельцем личного ключа электронной цифровой подписи (далее – личный ключ), на

- **Настоящий Закон направлен на установление правовых основ применения электронных документов**, определение основных требований, предъявляемых к электронным документам, **а также правовых условий использования электронной цифровой подписи в электронных документах**, при соблюдении которых электронная цифровая подпись в электронном документе является равнозначной собственноручной подписи в документе на бумажном носителе.
- https://www.oac.gov.by/public/content/files/files/law/laws-rb/113-z.pdf



Электронная подпись

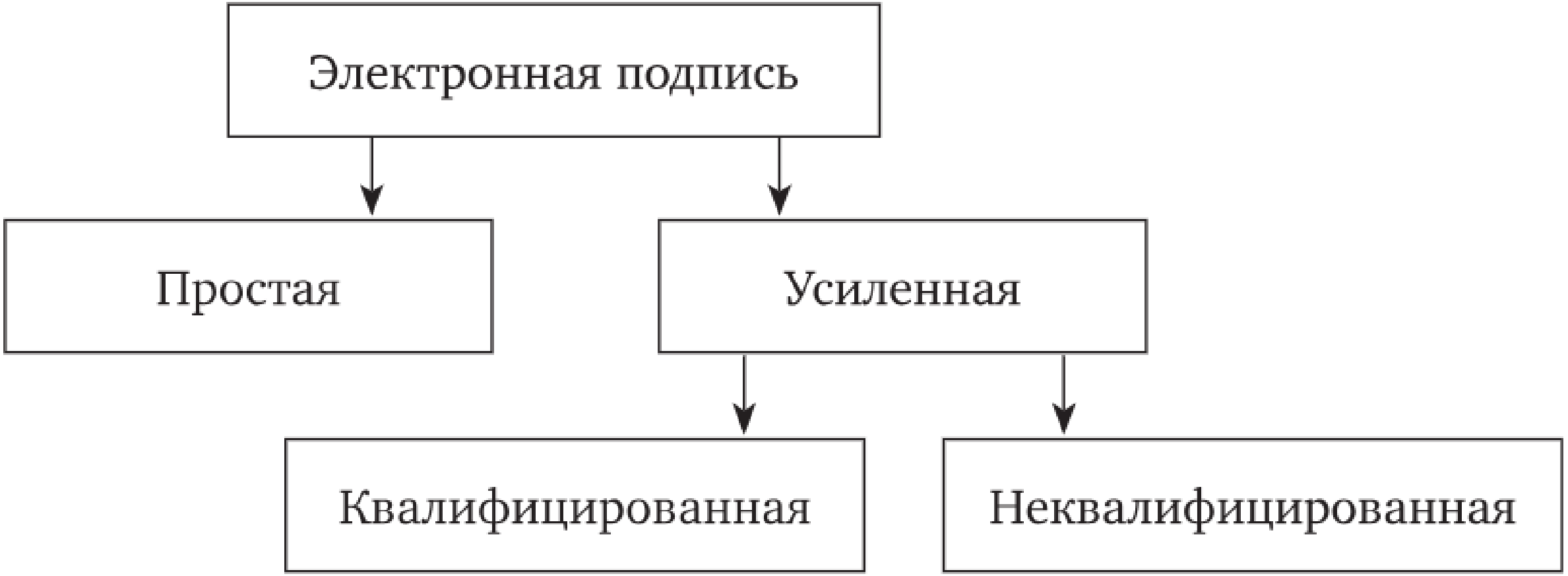
(ЦП – цифровая подпись)
(ЭЦП – электронная цифровая подпись)

Электронная подпись

https://ru.wikipedia.org/wiki/**Электронная_подпись**

- **Электронная подпись (ЭП), Электронная цифровая подпись (ЭЦП), Цифровая подпись (ЦП)** позволяет подтвердить авторство электронного документа (будь то реальное лицо или, например, аккаунт в криптовалютной системе). Подпись связана как с автором, так и с самим документом с помощью криптографических методов, и не может быть подделана с помощью обычного копирования.
- **ЭЦП** — это реквизит электронного документа, полученный в результате криптографического преобразования информации с использованием закрытого ключа подписи и позволяющий проверить отсутствие искажения информации в электронном документе с момента формирования подписи (целостность), принадлежность подписи владельцу сертификата ключа подписи (авторство), а в случае успешной проверки подтвердить факт подписания электронного документа (неотказуемость).

Типы электронной подписи



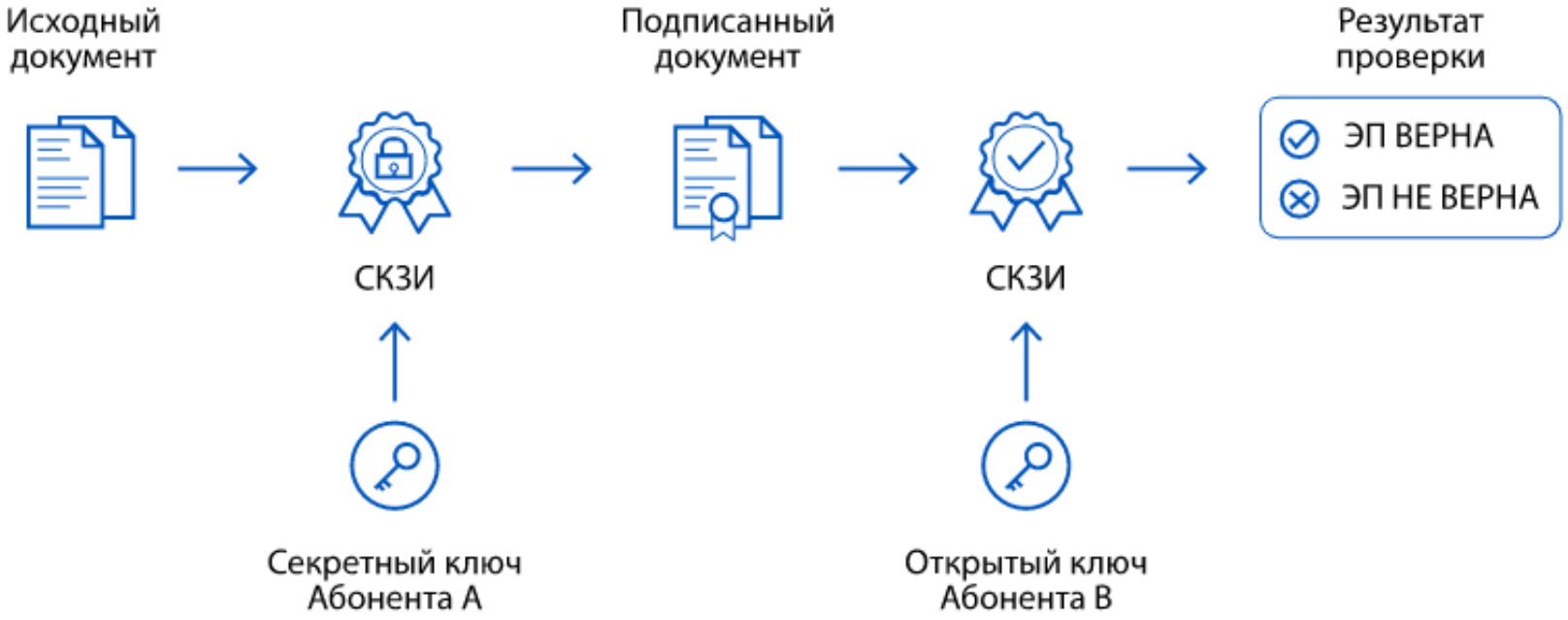
ЭЦП

Средство криптографической защиты информации

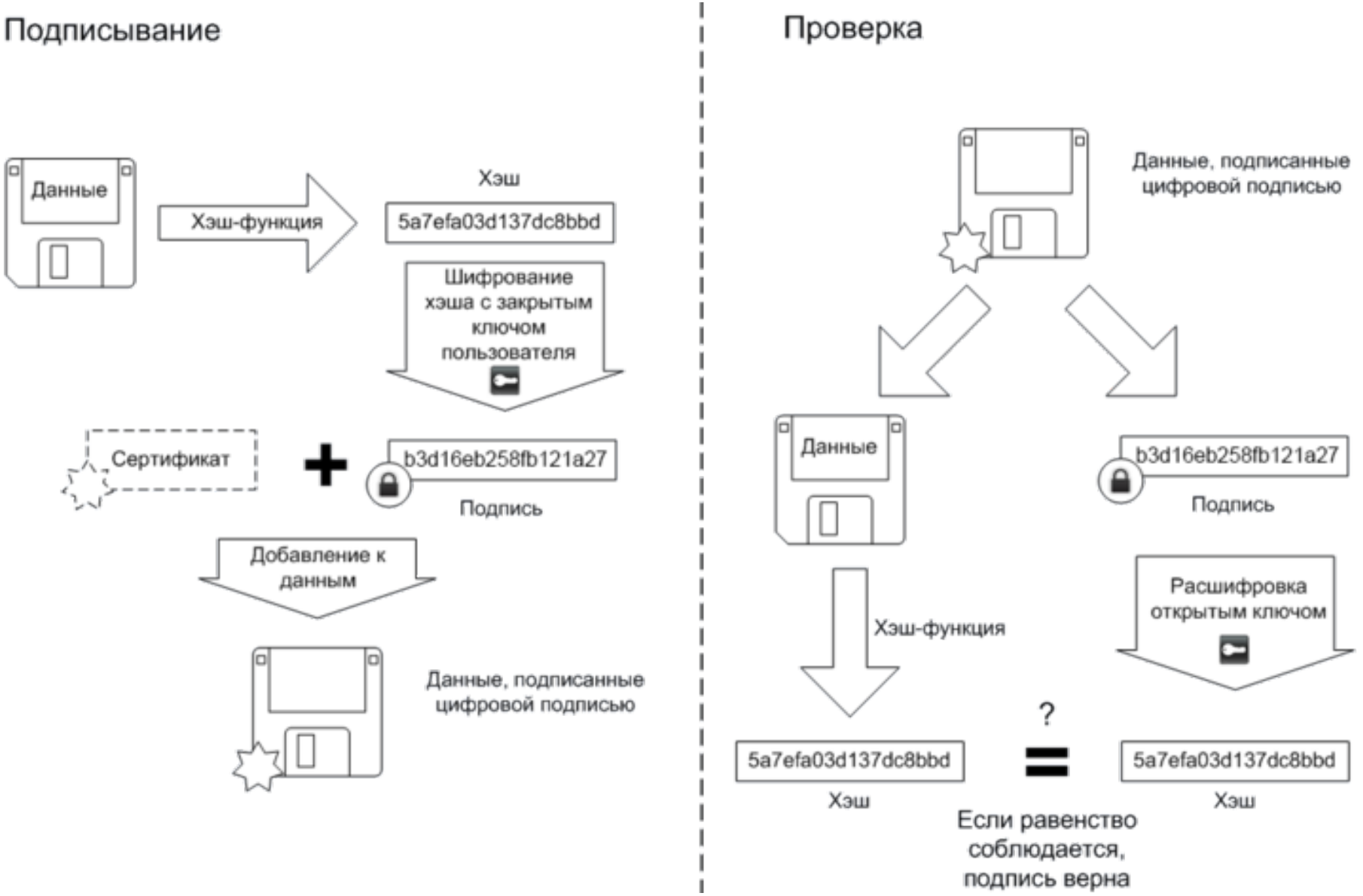
- **СКЗИ (средство криптографической защиты информации)** — это программа или устройство, которое шифрует документы и генерирует электронную подпись (ЭП).
- Все операции производятся с помощью ключа электронной подписи, который невозможно подобрать вручную, так как он представляет собой сложный набор символов. Тем самым обеспечивается надежная защита информации.

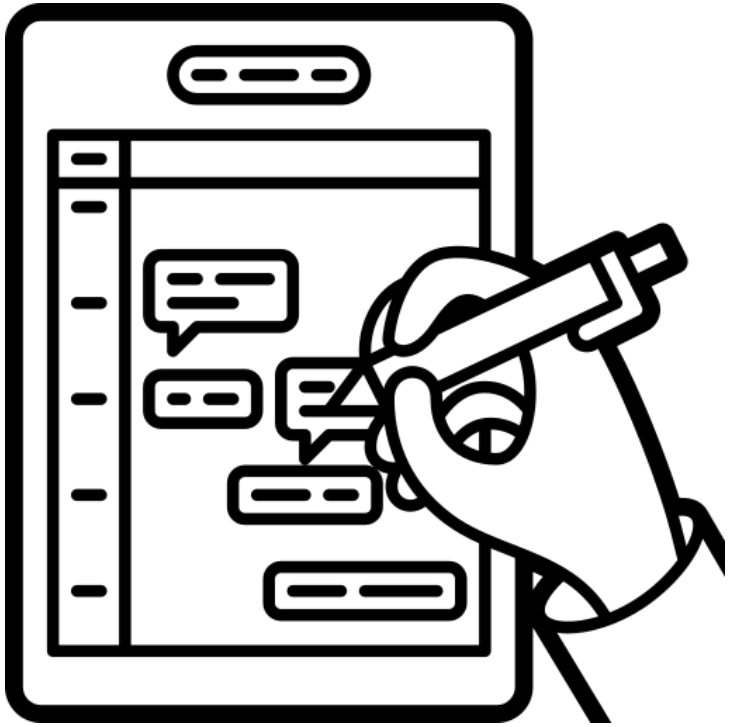
Принцип работы СКЗИ с ЭП

1. Отправитель создает документ
2. При помощи СКЗИ и закрытого ключа электронной подписи (ЭП) добавляет файл подписи, зашифровывает документ и объединяет все в файл, который отправляется получателю
3. Файл передается получателю
4. Получатель расшифровывает документ, используя СКЗИ и закрытый ключ своей электронной подписи
5. Получатель проверяет целостность ЭП, убеждаясь, что в документ не вносились изменения



Схема, поясняющая алгоритмы подписи и проверки





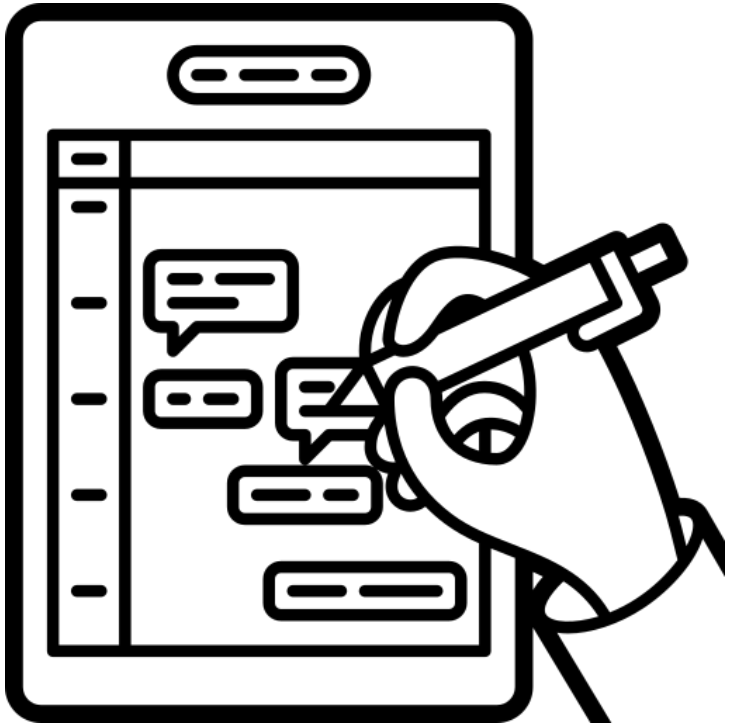
Алгоритмы электронно-цифровой подписи

Перечень алгоритмов ЭП

- **Асимметричные схемы:**
  - FDH (Full Domain Hash), вероятностная схема RSA-PSS (Probabilistic Signature Scheme), схемы стандарта PKCS#1 и другие схемы, основанные на алгоритме RSA
  - Схема Эль-Гамаля
  - Американские стандарты электронной цифровой подписи: DSA, ECDSA (DSA на основе аппарата эллиптических кривых)
  - Российские стандарты электронной цифровой подписи: ГОСТ Р 34.10-94 (в настоящее время не действует), ГОСТ Р 34.10-2001 (не рекомендован к использованию после 31 декабря 2017 года), ГОСТ Р 34.10-2012 (основан на сложности вычисления дискретного логарифма в группе точек эллиптической кривой)
  - Евразийский союз: ГОСТ 34.310-2004 полностью идентичен российскому стандарту ГОСТ Р 34.10-2001
  - Украинский стандарт электронной цифровой подписи ДСТУ 4145-2002
  - Белорусский стандарт электронной цифровой подписи СТБ 1176.2-99 (в настоящее время не действует), СТБ 34.101.45-2013
  - Схема Шнорра
  - Pointcheval-Stern signature algorithm
  - Вероятностная схема подписи Рабина
  - Схема BLS (Boneh-Lynn-Shacham)
  - Схема DLR (Donna-Lynn-Rivest)
  - Схема GMR (Goldwasser-Micali-Rivest)

Перечень алгоритмов ЭП

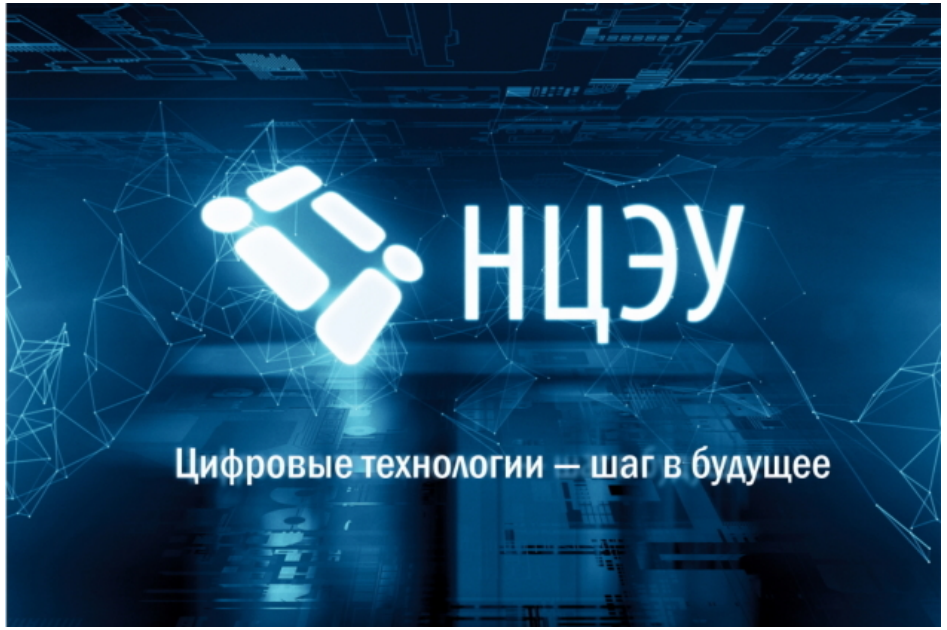
- На основе асимметричных схем созданы модификации цифровой подписи, отвечающие различным требованиям:
  - Групповая цифровая подпись
  - Неоспоримая цифровая подпись
  - «Слепая» цифровая подпись и справедливая «слепая» подпись
  - Конфиденциальная цифровая подпись
  - Цифровая подпись с доказуемостью подделки
  - Доверенная цифровая подпись
  - Разовая цифровая подпись



Организация хранение документов с электронно-цифровой подписью

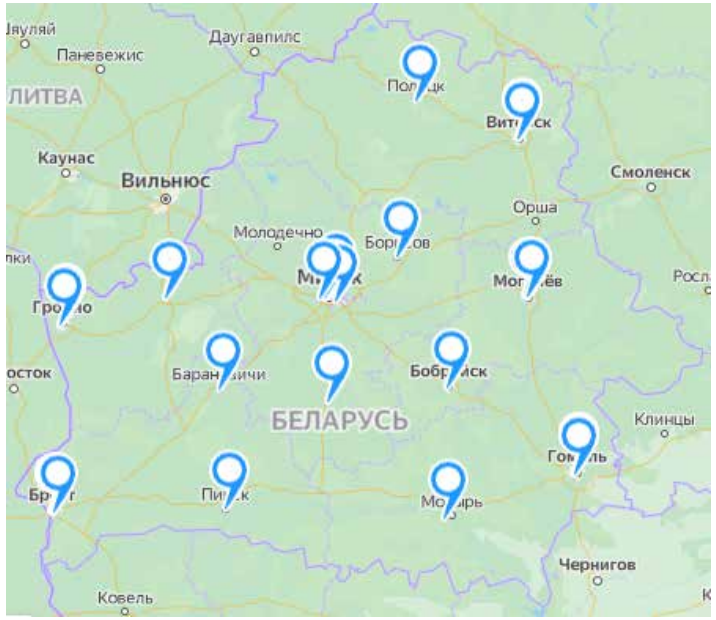
Электронная идентификация в Республике Беларусь https://nces.by/

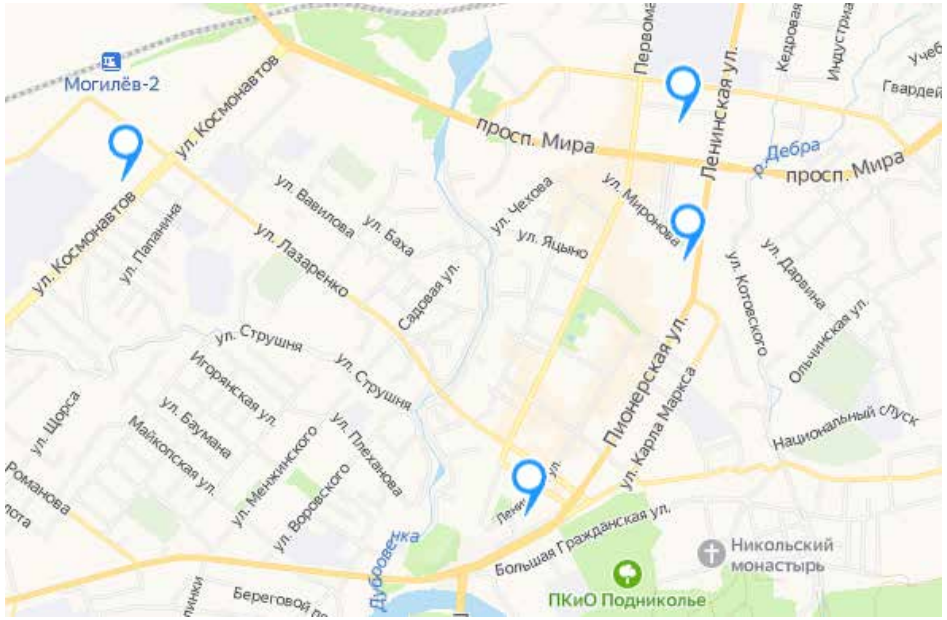
- **Национальный центр электронных услуг** — динамично развивающееся предприятие, выступающее инфраструктурным оператором важнейших межведомственных информационных систем, составляющих **фундамент электронного правительства в Республике Беларусь**.



Электронная идентификация НЦЭУ

- **НЦЭУ предлагает современные средства идентификации для юридически значимого обмена электронными документами.** Средства электронной цифровой подписи, которые используются сегодня **для работы в 30 информационных системах** — от регистрации предприятий и индивидуальных предпринимателей до подачи налоговых деклараций — можно получить в **45 точках оказания услуг.**





Перечень систем, использующих сертификаты РУЦ ГосСУОК

1. Ведомственные системы электронного документооборота (СЭД) во взаимодействии с системой межведомственного электронного документооборота государственных органов Республики Беларусь (СМДО).
2. Общегосударственная автоматизированная информационная система (ОАИС) для работы с Единым порталом электронных услуг для граждан и организаций (ЕПЭУ) (ВНИМАНИЕ! Авторизация на портале https://platform.gov.by с помощью мобильной ЭЦП не предусмотрена).
3. Единая информационная система государственной статистики Республики Беларусь (ЕИСГС) для обеспечения возможности представления респондентами государственной статистической отчетности.
4. Автоматизированная информационная система «Взаимодействие» Министерства юстиции Республики Беларусь для регистрации новых предприятий и индивидуальных предпринимателей.
5. Автоматизированные информационные системы Министерства по налогам и сборам Республики Беларусь (МНС): Портал «Электронные счета-фактуры» (Портал ЭСЧФ*; Инструкции) (ВНИМАНИЕ! Авторизация на портале ЭСЧФ с помощью мобильной ЭЦП не предусмотрена);
   Личный кабинет плательщика. (Авторизация с использованием ЭЦП доступна физическим и юридическим лицам, а также индивидуальным предпринимателям. Авторизация по мобильной ЭЦП доступна только физическим лицам и индивидуальным предпринимателям).
6. Информационный ресурс «Единая информационная база данных контролирующих (надзорных) органов, включающая сведения о проверяемых субъектах и об отнесении их к соответствующим группам риска исходя из критериев отнесения проверяемых субъектов к группе риска для назначения плановых проверок» (АИС КНО).
7. Системы Фонда социальной защиты населения для представления отчетной информации (Портал ФСЗН; получить атрибутный сертификат для работы с системами ФСЗН).
8. Информационная система электронного декларирования таможенных органов Республики Беларусь.
9. Информационная система «Уведомительное декларирование соответствия» для регистрации в Республике Беларусь деклараций о соответствии продукции требованиям технических регламентов Таможенного союза в электронной форме.
10. Ведомственные автоматизированные информационные системы для подготовки и отправки отчетности в Департамент финансового мониторинга КГК (Белорусская нотариальная палата; ИП, оказывающие юридические услуги и др.).
11. Единый государственный регистр недвижимого имущества, прав на него и сделок с ним (ЕГРНИ).

Защита информации

Тема: Электронная цифровая подпись

Благодарю за внимание

КУТУЗОВ Виктор Владимирович

Белорусско-Российский университет, Кафедра «Программное обеспечение информационных технологий»
Республика Беларусь, Могилев, 2024