Московский институт электроники и математики им. А.Н. Тихонова

Кафедра информационной безопасности киберфизических систем

Москва 2024

Криптографические методы защиты информации

Электронная подпись

Общие сведения

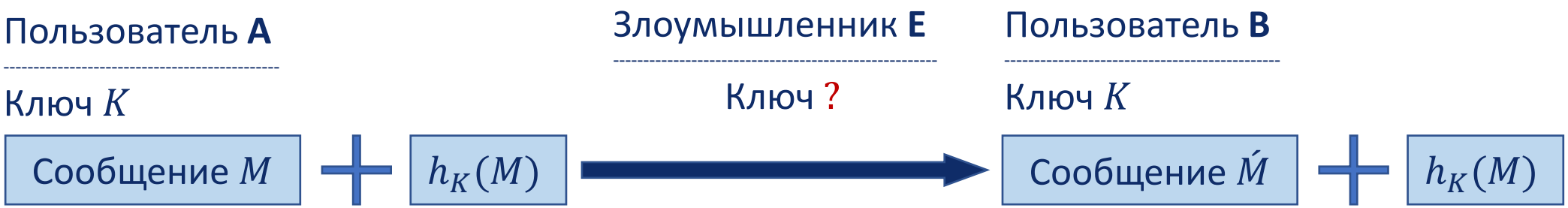
Методы обеспечения контроля целостности данных

- **Хэширование**

Защита от случайных искажений

Методы обеспечения контроля целостности данных

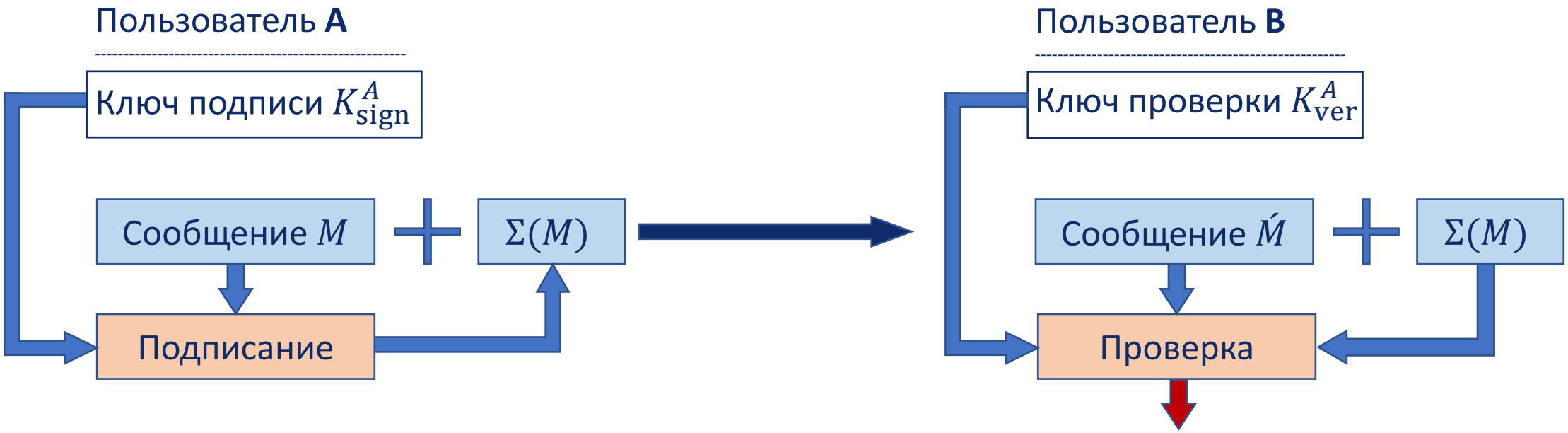
- **Код аутентичности сообщения (имитовставка)**



Защита от внешнего злоумышленника

Методы обеспечения контроля целостности данных

- **Электронная подпись**



Защита от ренегатства

Определения понятия «электронная подпись»

- **Электронная подпись** — это информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию (ФЗ «Об электронной подписи»).
- **Электронная подпись сообщения** — это некоторая битовая строка, зависящая от самого сообщения и секретного ключа, известного только автору подписи, и позволяющая установить авторство сообщения и/или опровергнуть подделку.

Виды электронной подписи

- Федеральный закон от 06.04.2011 N 63-ФЗ «Об электронной подписи»:
  - **Простая электронная подпись** — основана на использовании кодов, паролей или иных средств.
  - **Усиленная электронная подпись** — основана на криптографическом преобразовании информации с использованием ключа электронной подписи:
    - усиленная неквалифицированная электронная подпись;
    - усиленная квалифицированная электронная подпись.

Стандарты электронной подписи

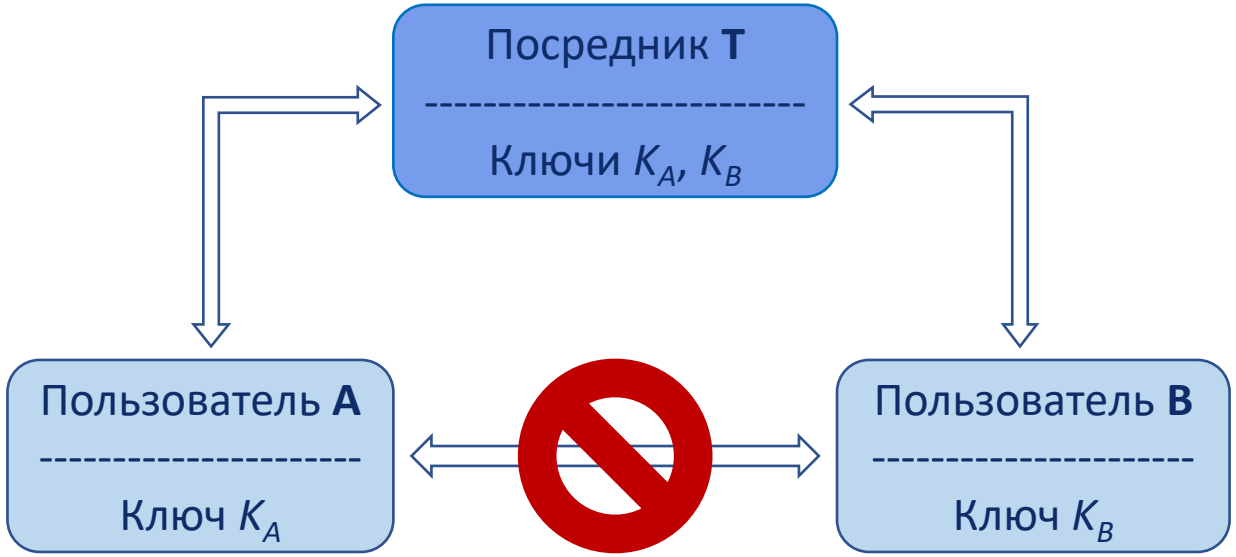
- Российская Федерация:
  - **ГОСТ Р 34.10-2012.** Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи.
- США:
  - **FIPS PUB 186-5**. Digital Signature Standard (DSS):
    - **RSA Digital Signature Algorithm (RSA DSA)**;
    - Elliptic Curve Digital Signature Algorithm (ECDSA);
    - Edwards Curve Digital Signature Algorithm (EdDSA).

Способы построения схем электронной подписи

Построение схем электронной подписи на основе симметричных и асимметричных алгоритмов

- На основе **симметричных алгоритмов**:
  - Подписание сообщения заключается в его зашифровании с помощью симметричного шифра.
  - Пользователи не обмениваются сообщениями напрямую, а используют доверенную третью сторону.
- На основе **асимметричных алгоритмов**:
  - Каждый пользователь обладает ключевой парой, где закрытый ключ является ключом подписи, а открытый ключ – ключом проверки подписи.
  - Для подтверждения подлинности открытых ключей используется доверенная третья сторона.

Схема электронной подписи на симметричной криптографии



Асимметричные схемы электронной подписи

Схема электронной подписи на основе криптосистемы RSA

1. Алиса формирует сообщение m.
2. Алиса выполняет преобразование

$$s = m^d \pmod{n}.$$

3. Алиса передает Бобу пару (m, s).
4. Боб получает сообщение Алисы и выполняет преобразование

$$m' = s^e \pmod{n}.$$

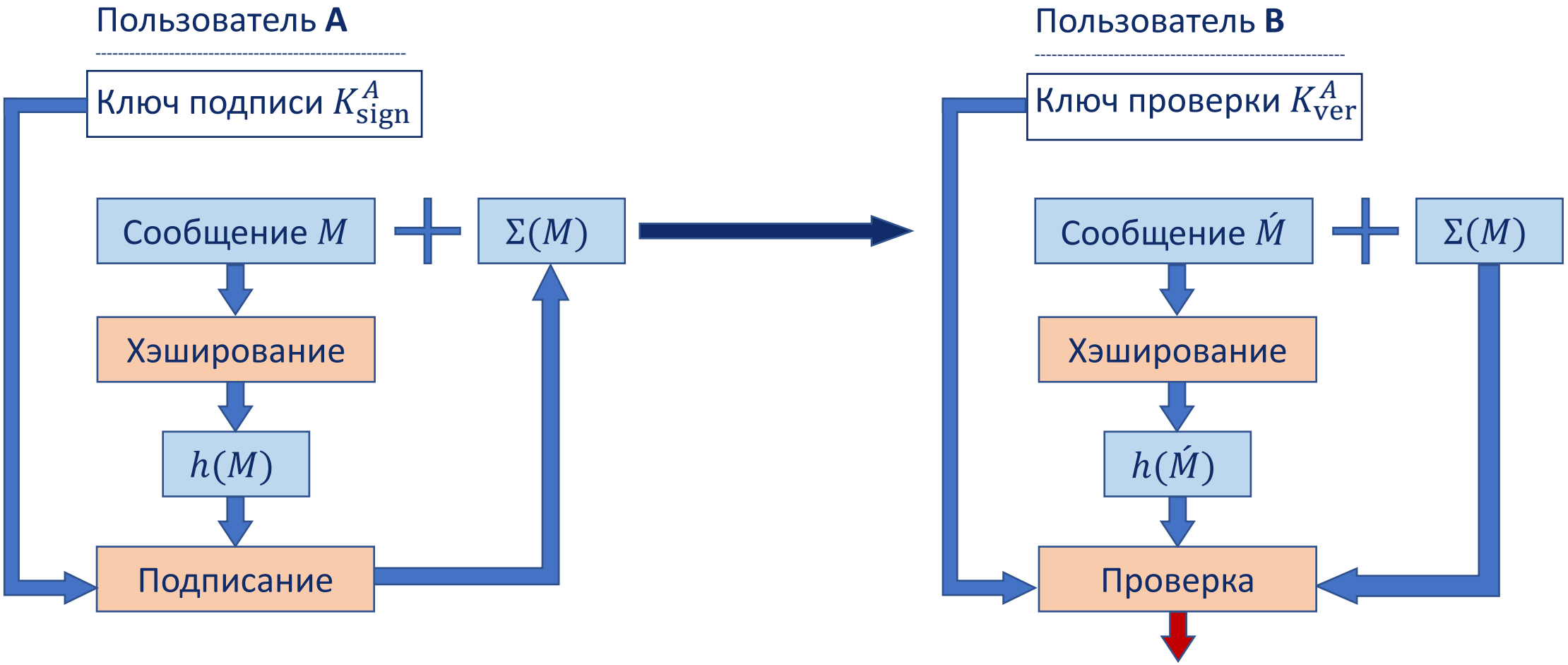
5. Если $m' = m$, то подпись верна.

Схема электронной подписи Эль-Гамаля

1. Алиса формирует сообщение m.
2. Алиса выбирает сеансовый ключ k в интервале $1 < k < p - 1$ и вычисляет $r = g^k \pmod p$.
3. Алиса вычисляет два числа:
   - $u = (m - xr) \pmod{p - 1}$;
   - $s = k^{-1}u \pmod{p - 1}$, где k^{-1}: $k^{-1}k \equiv 1 \pmod{p - 1}$.
4. Алиса передает Бобу тройку (m, r, s).
5. Боб получает сообщение Алисы и выполняет проверку равенства
   - $h^r r^s = g^m \pmod p$.
6. Если равенство выполняется, то подпись верна.

Уточненная схема электронной подписи

Уточненная схема электронной подписи



Спасибо за внимание!

Евсютин Олег Олегович
Заведующий кафедрой информационной безопасности киберфизических систем
Канд. техн. наук, доцент

+7 923 403 09 21
oevsyutin@hse.ru