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

Кафедра информационной безопасности киберфизических систем

Москва 2024

Криптографические методы защиты информации

Введение в дисциплину

Организация курса

Преподаватели

Евсютин Олег Олегович – заведующий кафедрой информационной безопасности киберфизических систем Московского института электроники и математики им. А.Н. Тихонова Национального исследовательского университета «Высшая школа экономики», кандидат технических наук, доцент, специалист в области кибербезопасности, цифровой стеганографии, цифровых водяных знаков.

https://www.hse.ru/org/persons/304056117

+7 923 403 09 21

oevsyutin@hse.ru

Преподаватели

Мельман Анна Сергеевна – младший научный сотрудник кафедры информационной безопасности киберфизических систем Московского института электроники и математики им. А.Н. Тихонова Национального исследовательского университета «Высшая школа экономики», специалист в области кибербезопасности, цифровой стеганографии, цифровых водяных знаков.

https://www.hse.ru/org/persons/446743910

+7 923 434 11 18

amelman@hse.ru

Содержание курса

Общие сведения о криптографии

Математические основы современной криптографии

- Высшая алгебра
- Теория чисел

Криптографические методы и алгоритмы

- Историческая криптография
- Симметричные шифры
- Криптография с открытым ключом
- Хеширование
- Электронная подпись
- Инфраструктура открытого ключа
- Квантовая криптография

Текущий контроль

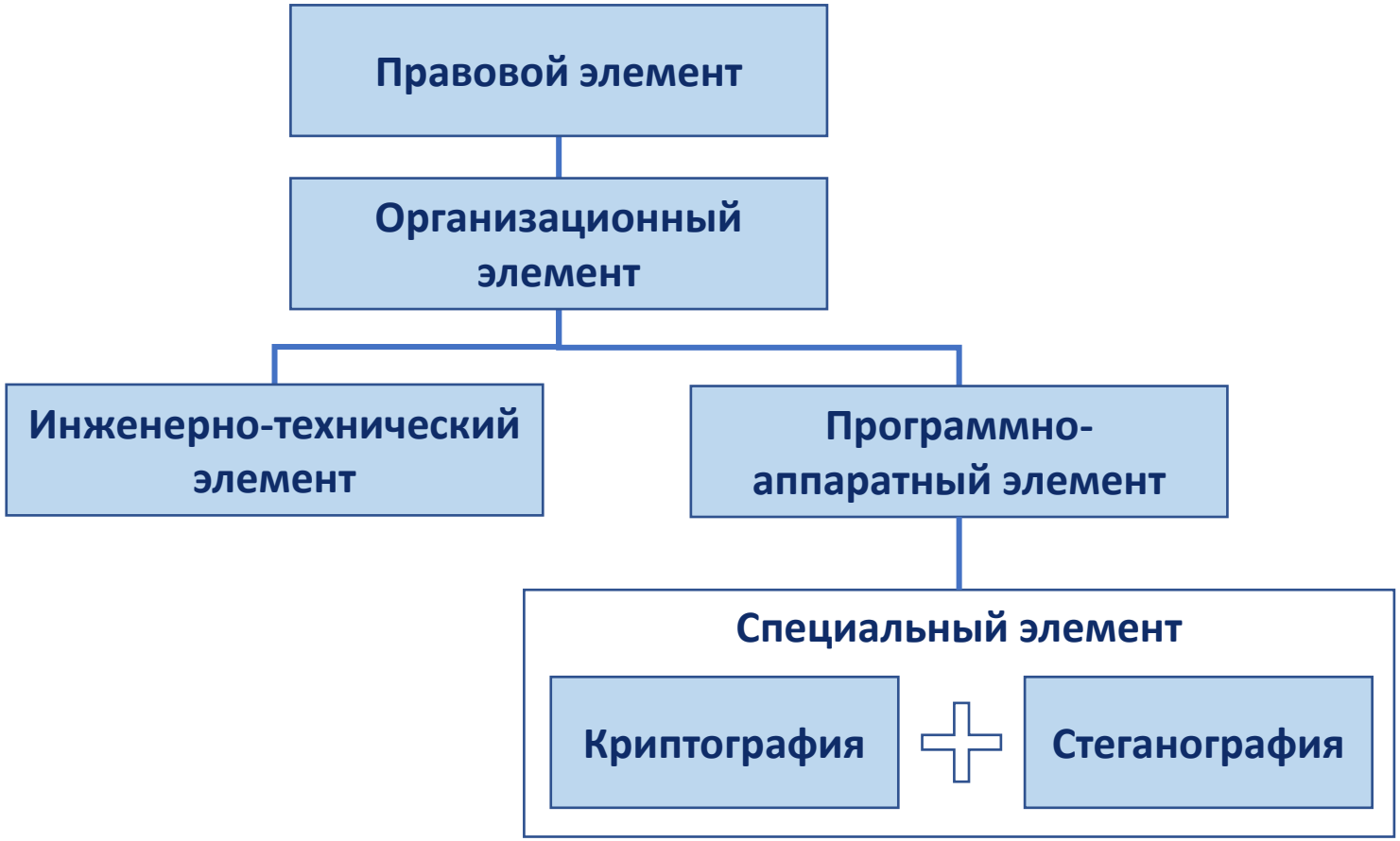
Раздел курса	Контрольные работы	Практические работы	Тест
Высшая алгебра	1	3	—
Теория чисел	1		—
Криптографические методы и алгоритмы	—		1

Формула оценивания:

0.3 * Контрольные работы + 0.3 * Практические работы + 0.1 * Тест + 0.3 * Экзамен

Основы криптографии

Комплекс мер по обеспечению информационной безопасности



Основные понятия и определения

- **Криптография** — это наука о математических методах преобразования информации с целью ее защиты.
- **Криптоанализ** — это наука, занимающаяся исследованием методов получения доступа к зашифрованной информации без знания секретного ключа. Кроме того, под криптоанализом понимается любая попытка найти уязвимость в криптографическом алгоритме или протоколе.
- Отрасль математики, включающая в себя криптографию и криптоанализ, называется **криптологией**.

Основные задачи криптографии

Криптографические методы защиты информации:

- шифрование,
- хеширование,
- имитовставка,
- электронная подпись.

Задачи криптографии:

- обеспечение конфиденциальности информации,
- обеспечение контроля целостности информации,
- обеспечение аутентификации данных и источника данных,
- обеспечение возможности подтверждения авторства и невозможности отказа от авторства.

Математический аппарат

Абстрактная алгебра:

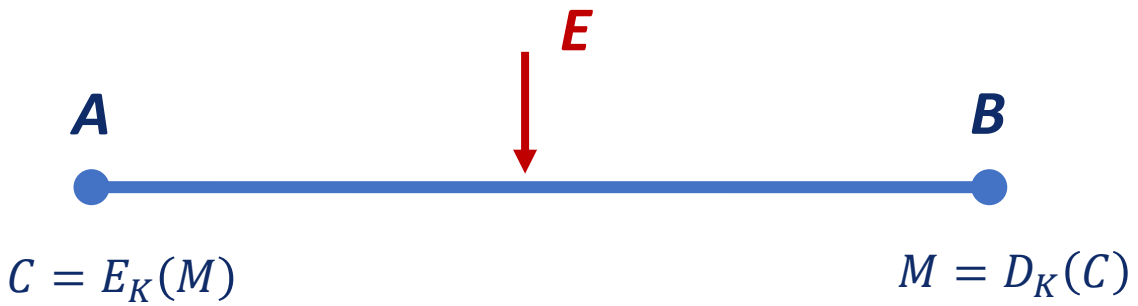
- алгебраические структуры;
- циклические группы;
- кольца классов вычетов;
- кольца многочленов;
- конечные поля;
- эллиптические кривые.

Теория чисел:

- простые числа;
- арифметика остатков;
- целочисленная факторизация и дискретное логарифмирование.

Шифрование

- **Шифрование** направлено на обеспечение секретности информации, передаваемой по открытым каналам связи.
- Основные понятия:
  - открытый текст M;
  - шифртекст (криптограмма) C;
  - зашифрование E;
  - расшифрование D;
  - ключ K.



A, ***B***: законные пользователи

E: злоумышленник

Расшифрование $\neq$ дешифрование

Шифрование

- **Шифром** (**криптосистемой**) называют совокупность криптографических алгоритмов зашифрования и расшифрования вместе с алгоритмами генерации соответствующих ключей.
- **Ключ** — это секретный элемент данных, знание которого позволяет законному пользователю осуществлять зашифование и расшифрование данных, и незнание которого не позволяет злоумышленнику прочитать зашифрованные данные.

Классификация современных шифров:

- **симметричные** шифры:
  - блочные,
  - поточные,
- **асимметричные** шифры.

Хеширование

- **Хеширование** — это преобразование входной битовой строки произвольной длины в выходную битовую строку фиксированной длины.
- Хеш-функция: сообщение → хеш-код.
- Хеширование предназначено для обеспечения контроля целостности информации.

Пример хеширования текста

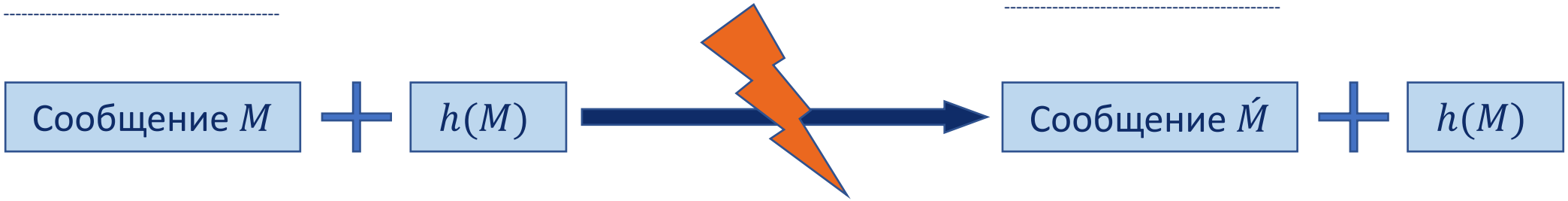
Национальный исследовательский университет «Высшая школа экономики» — исследовательский университет, осуществляющий свою миссию через научно-образовательную, проектную, экспертно-аналитическую и социокультурную деятельности на основе международных научных и организационных стандартов.	Национальный исследовательский университет «Высшая Школа Экономики» — исследовательский университет, осуществляющий свою миссию через научно-образовательную, проектную, экспертно-аналитическую и социокультурную деятельности на основе международных научных и организационных стандартов.
6B4FD9F1D385D9FCCD7532ED1254B7B44EA1FBF76F8F9766DAE79F20C83AA619	F8A42D79D2AE48D6448CE589720A39E828277A76F35CD10B41F46DD75C6C20CB

Хеширование

Защита от случайных искажений

Пользователь **A**

Пользователь **B**

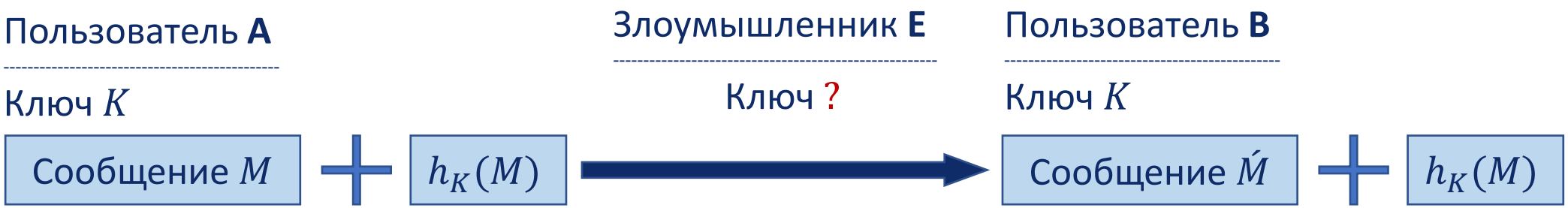


Если $\boldsymbol{h(\acute{M}) = h(M)}$, то:

- $\boldsymbol{\acute{M} = M}$.

Код аутентичности сообщения (имитовставка)

Защита от внешнего злоумышленника

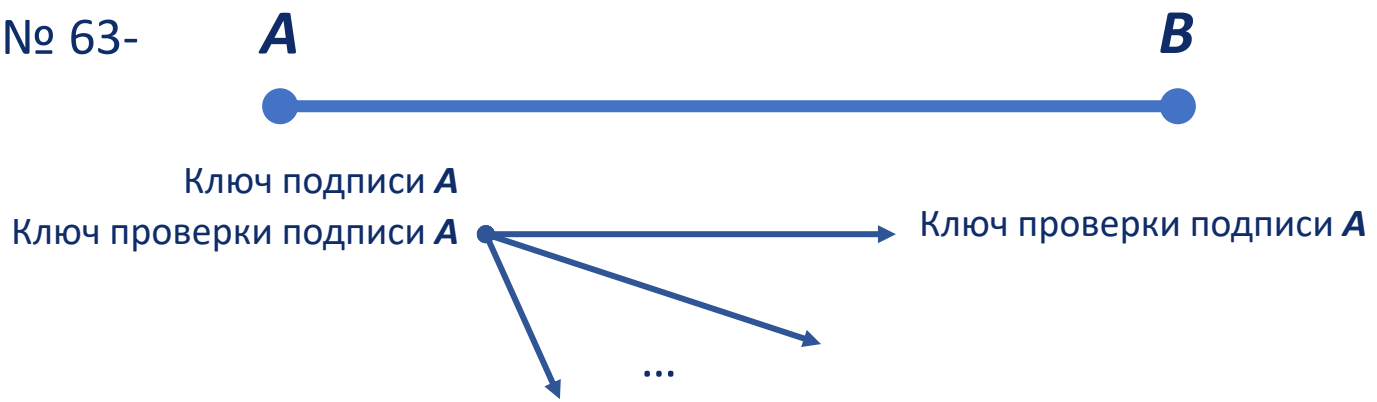


Если $\boldsymbol{h_K(\acute{M}) = h_K(M)}$, то:

- $\boldsymbol{\acute{M} = M}$;
- ***A*** – отправитель.

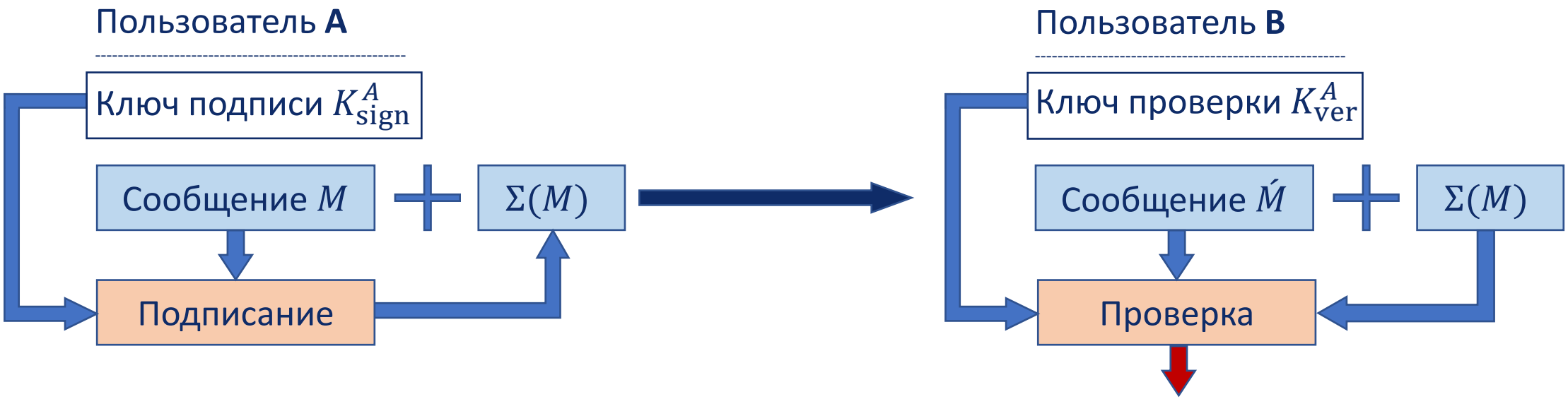
Электронная подпись

- **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 (Федеральный закон от 6 апреля 2011 г. № 63-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.



Электронная подпись

Защита от ренегатства



Если значение $\Sigma(M)$ корректно, то:

- $\boldsymbol{\acute{M} = M}$;
- ***A*** – автор и отправитель.

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

Кафедра информационной безопасности киберфизических систем

Криптографические методы защиты информации

Спасибо за внимание!

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

+7 923 403 09 21
oevsyutin@hse.ru