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

Кафедра информационной безопасности киберфизических систем

Москва 2024

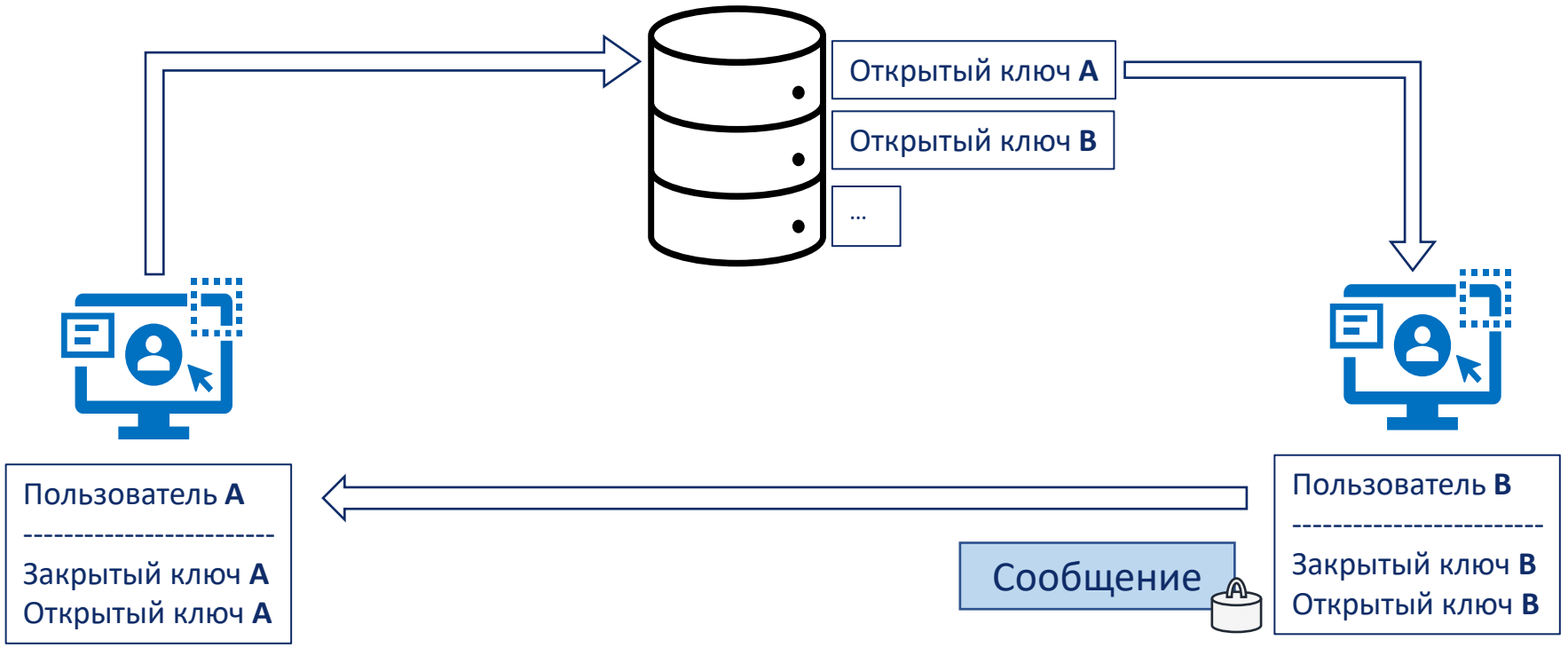
Криптографические методы защиты информации

Инфраструктура открытого ключа

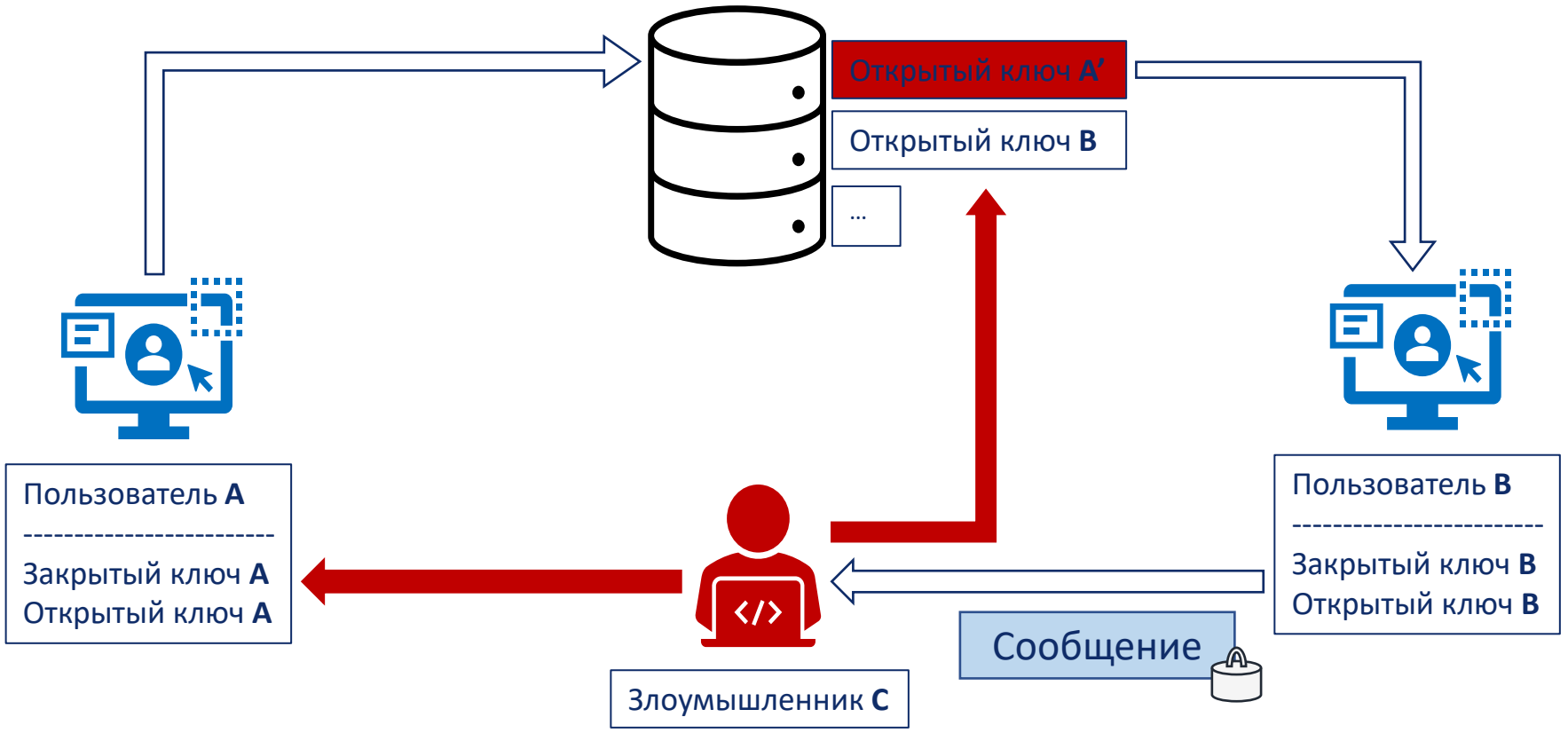
Применение асимметричной криптографии

- **Шифрование информации**:
  - Защита содержания электронных документов.
- **Формирование и проверка электронной подписи**:
  - Подписывание электронных документов.
  - Контроль доступа к данным.
  - Подтверждение личности пользователя.
  - Аутентификации данных.

Схема обмена открытыми ключами



Вмешательство злоумышленника в обмен открытыми ключами



Инфраструктура открытого ключа

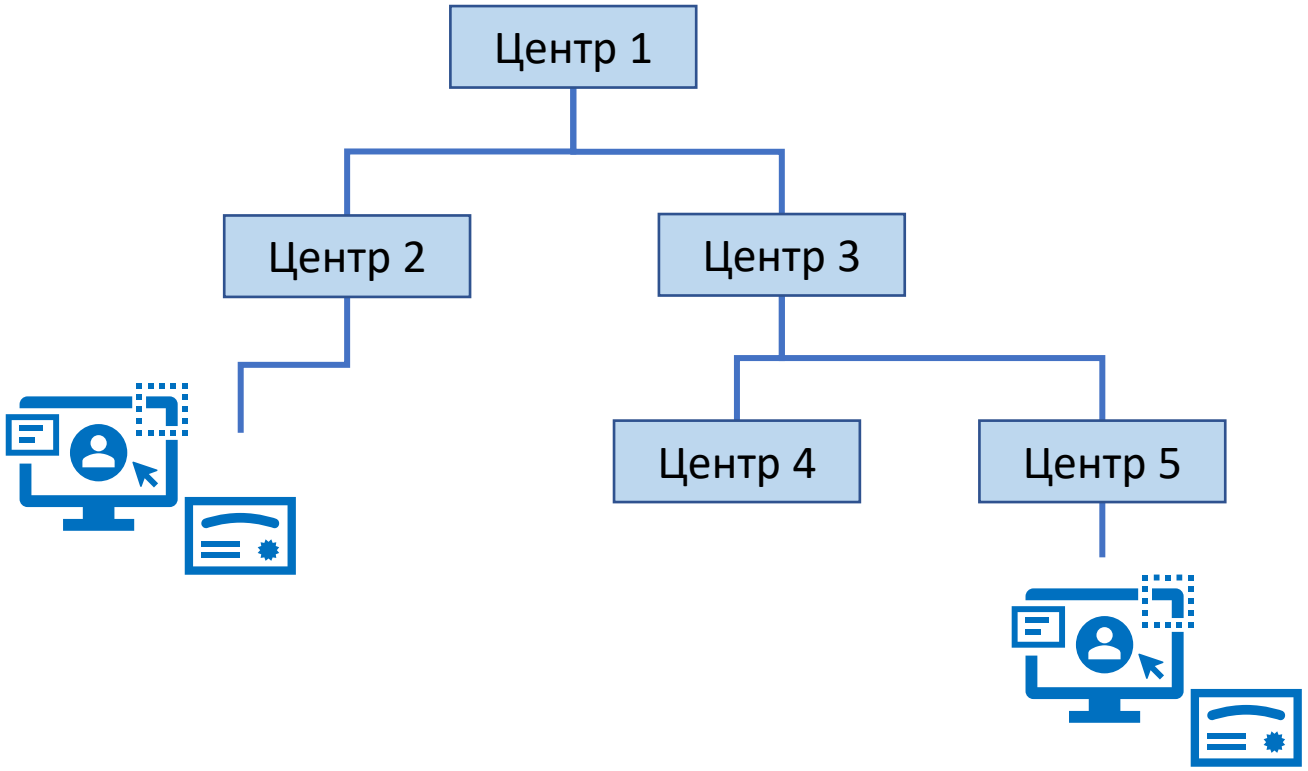
- **Инфраструктура открытого ключа** (Public Key Infrastructure — PKI) представляет собой систему, с помощью которой можно определить, кому принадлежит тот или иной открытый ключ.
- Процесс сопоставления открытого ключа физическому лицу или уполномоченному агенту называется **привязкой**.
- **Цифровой сертификат** — способ привязки, лежащий в основе инфраструктуры открытого ключа.
- **Центр сертификации** (**центр сертификатов**, **удостоверяющий центр**) — это центральный орган, служащий посредником между пользователями и удостоверяющий аутентичность их открытых ключей.

Центр сертификации

Стандарт X.509

- **Сертификат:**
  - Версия
  - Серийный номер
  - Идентификатор алгоритма подписи
  - Имя издателя
  - Период действия
  - Имя субъекта
  - Информация об открытом ключе субъекта:
    - Алгоритм открытого ключа
    - Открытый ключ субъекта
  - Уникальный идентификатор издателя (обязательно только для v2 и v3)
  - Уникальный идентификатор субъекта (обязательно только для v2 и v3)
  - Дополнения (для v2 и v3)
- **Алгоритм подписи сертификата (обязательно только для v3).**
- **Подпись сертификата.**

Цепочки сертификатов



Ограничения инфраструктуры открытого ключа

- Невозможность построения глобальной инфраструктуры.
  - Отсутствие единого центра сертификации.
  - Вопрос выбора имен пользователей.
  - Отзыв скомпрометированных сертификатов.
- **Список отзыва сертификатов** — сообщение, подписанное центром сертификации и содержащее серийные номера сертификатов, которые были отозваны этим центром, но чей срок действия еще не истек.

Спасибо за внимание!

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

+7 923 403 09 21
oevsyutin@hse.ru