Тема 7

Средства аутентификации при защите программного обеспечения и баз данных

Содержание темы

- Понятие идентификации и аутентификации.
- Классификация средств аутентификации при защите программного обеспечения и баз данных.
- Парольные средства аутентификации.
- Средства аутентификации с использованием смарт-карт и электронных ключей.
- Биометрические средства аутентификации.
- Протоколы сетевой аутентификации.

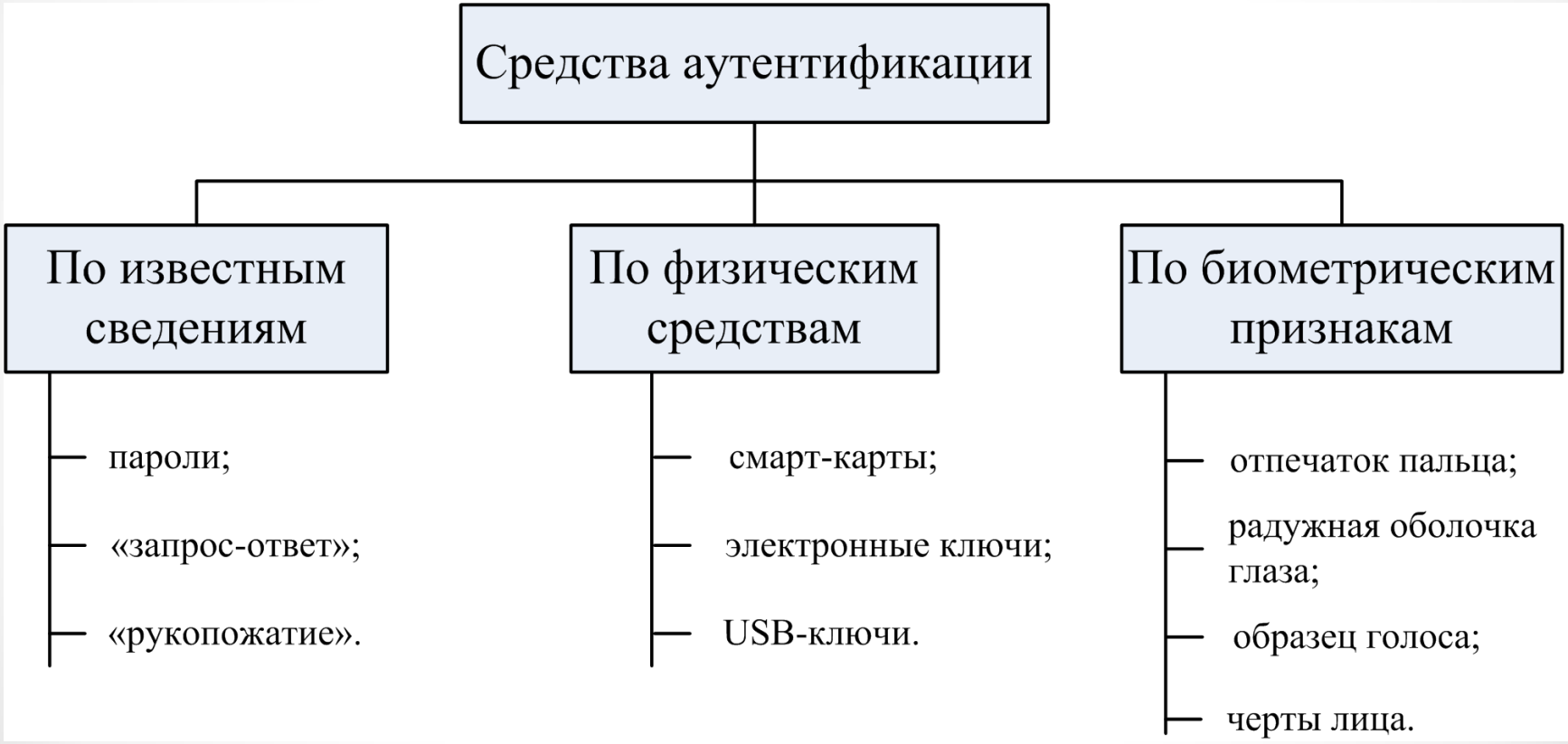
Идентификация и аутентификация

Идентификация – это процесс распознавания субъекта с помощью заранее присвоенного идентификатора.

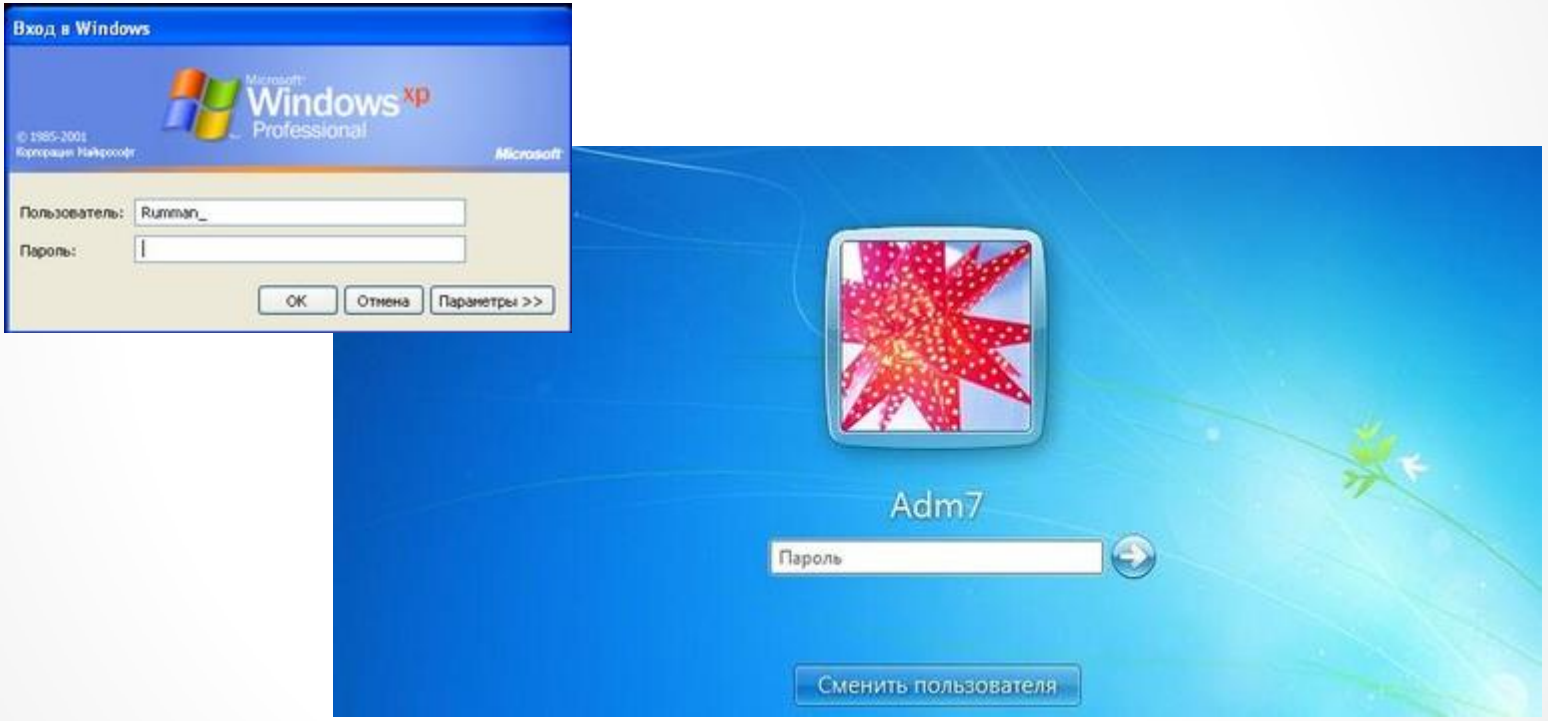
Аутентификация – это процесс, который обеспечивает проверку законности субъекта аутентификации и устанавливает, является ли он тем, за кого себя выдает.

Идентификация является частью аутентификации и заключается в работе с именем субъекта (логин).

Классификация средств аутентификации



Парольные средства аутентификации



Парольные средства аутентификации

Параметры пароля:

- A – алфавит пароля (набор символов, которые могут участвовать в образовании пароля);
- k – количество символов в пароле;
- A^k – количество вариантов возможных паролей.

A	k	A^k
Цифры (10)	4	10 000
Английские буквы (26)	5	11 881 376
Русские буквы (33)	7	42 618 442 977
Составной пароль (100)	10	10^{20}
Байты (256)	16	$3{,}4\times10^{38}$

Парольные средства аутентификации

Один из основных показателей эффективности парольных средств аутентификации:

Вероятность подбора пароля с первой попытки

$$P_{\text{па}1} = \frac{1}{A^k}$$

Парольные средства аутентификации

Недостатки парольных средств аутентификации:

- пароли должны быть надежными;
- необходимость периодической смены паролей;
- необходимость использования разных паролей для разных систем, требующих аутентификации.

Носимые средства аутентификации

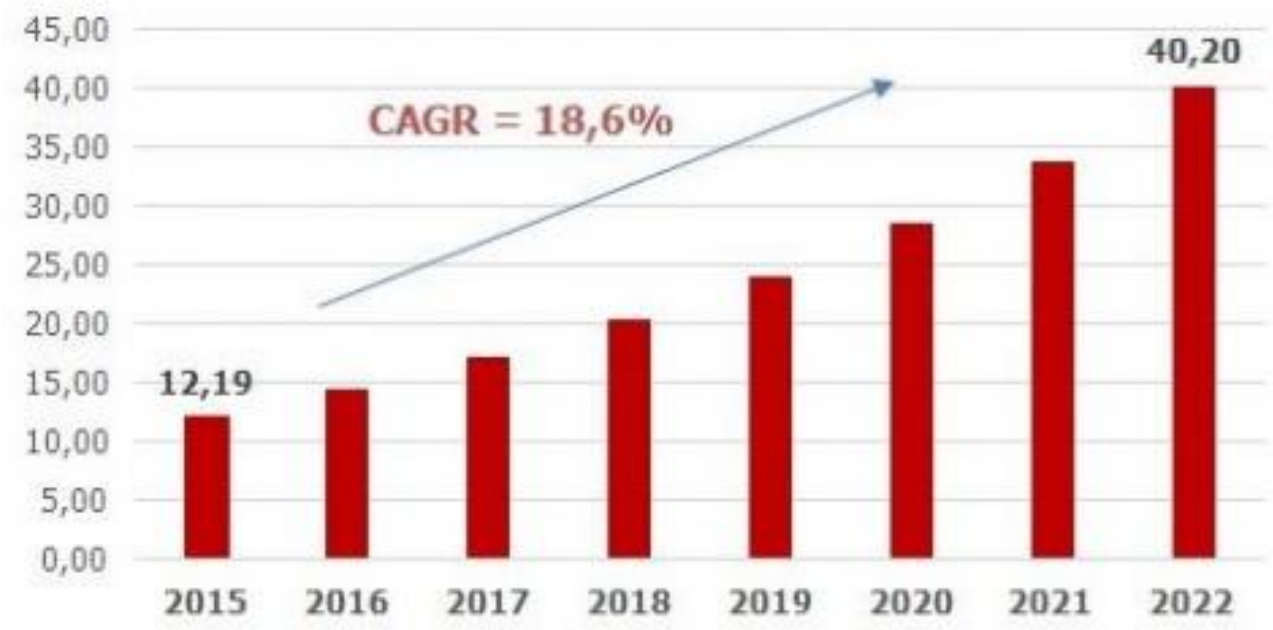
Электронный ключ (iButton)
48-битный код

Смарт-карта
код от 64 бит

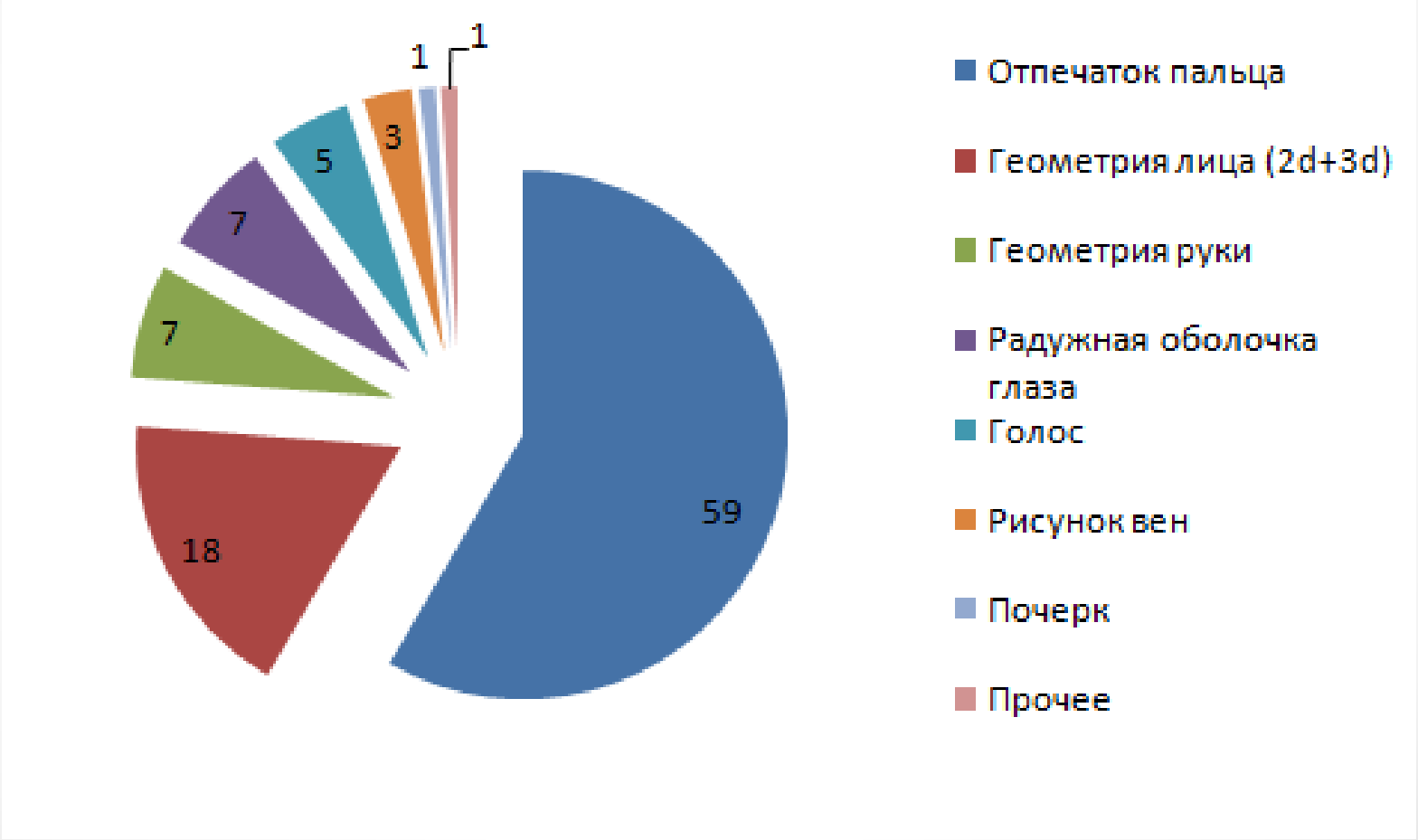
USB-ключ

Биометрия

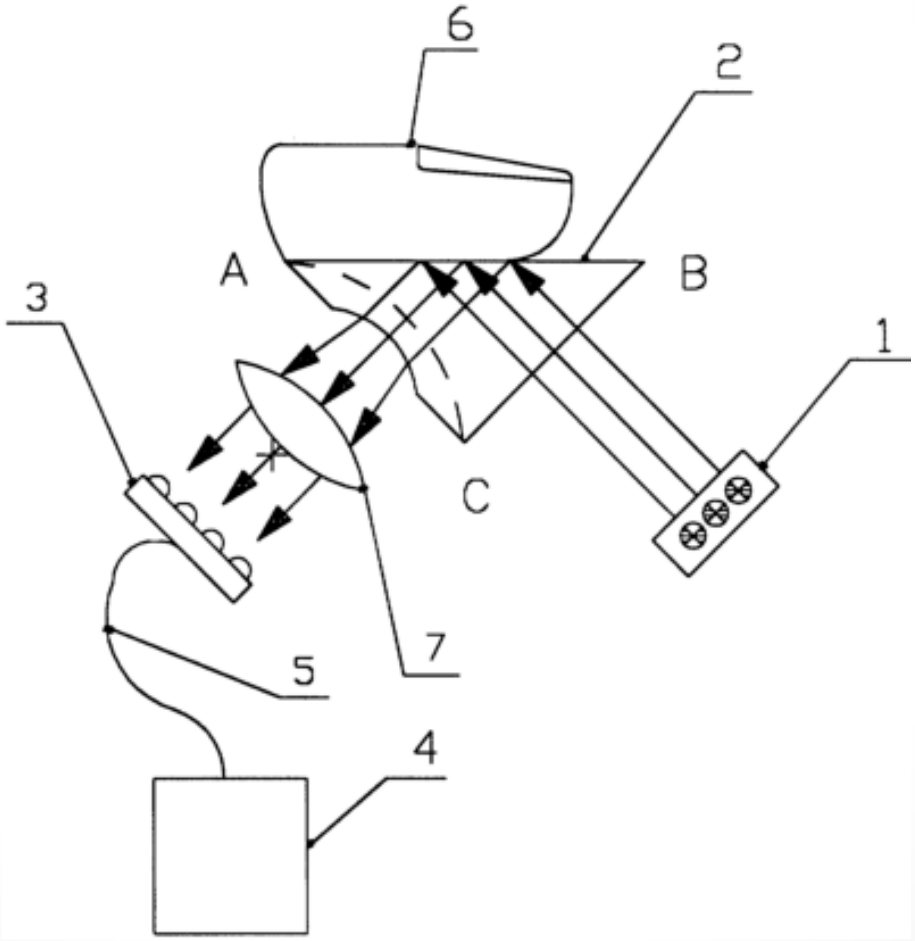
Рис. 1. Объем мирового рынка биометрических систем в 2015-2022 гг., $млрд.



Биометрия


59
18
7
7
5
3
1
1
Отпечаток пальца
Геометрия лица (2d+3d)
Геометрия руки
Радужная оболочка глаза
Голос
Рисунок вен
Почерк
Прочее

Биометрия

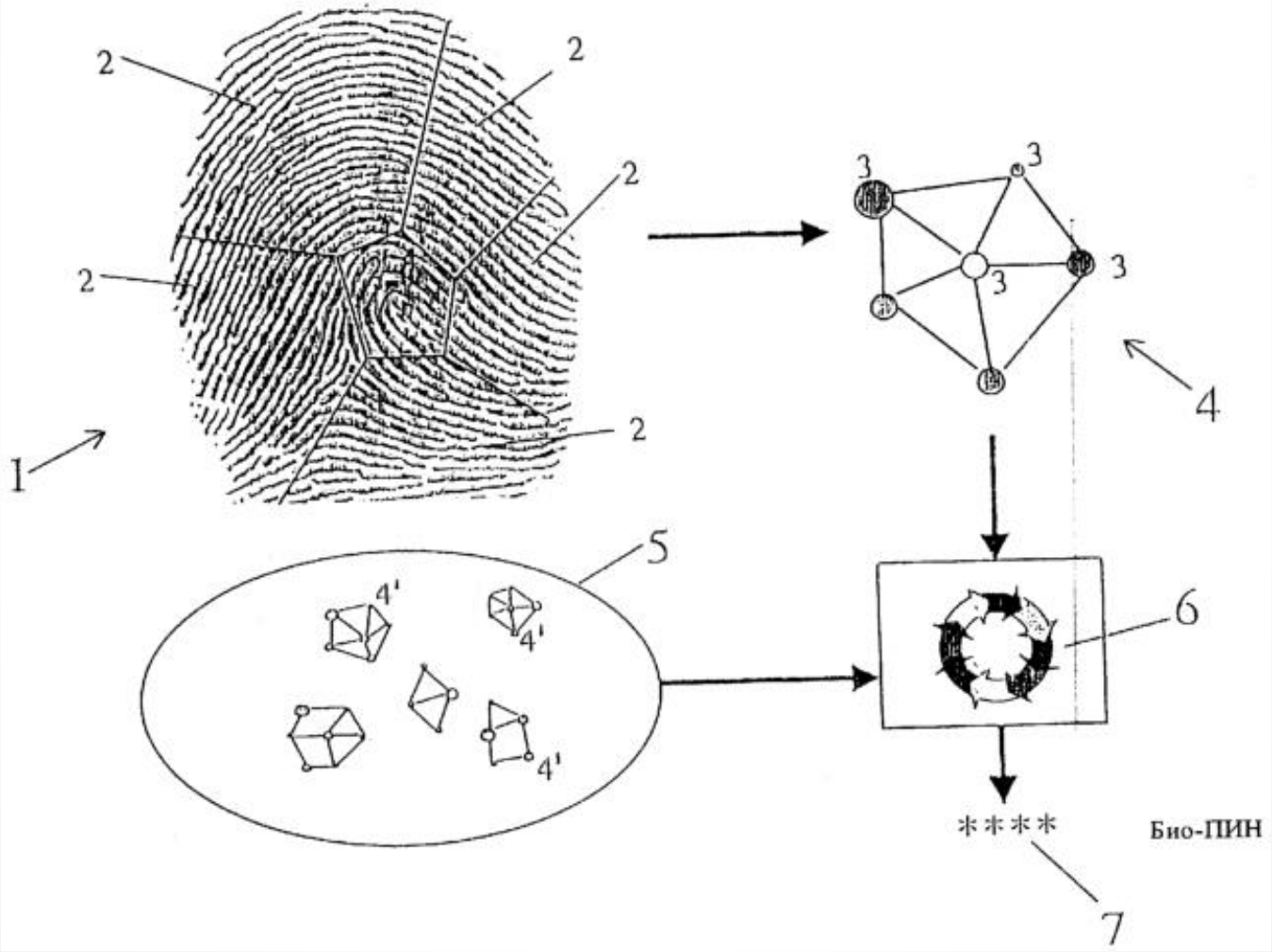


Биометрия

Папиллярные линии – рельефные линии на ладонных и подошвенных поверхностях.

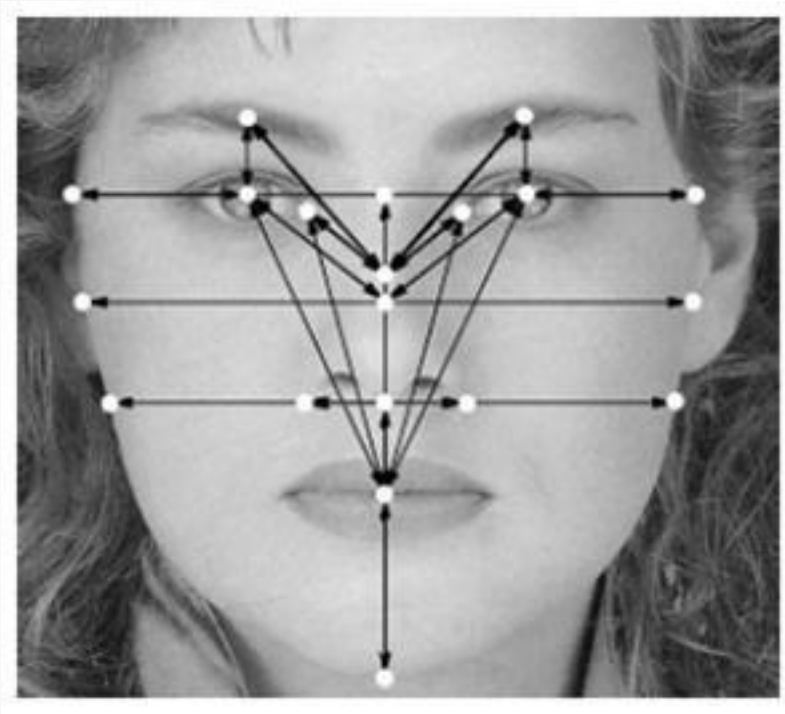
Минуции – участки папиллярного рисунка кожи, где отдельные линии сливаются, раздваиваются или обрываются.

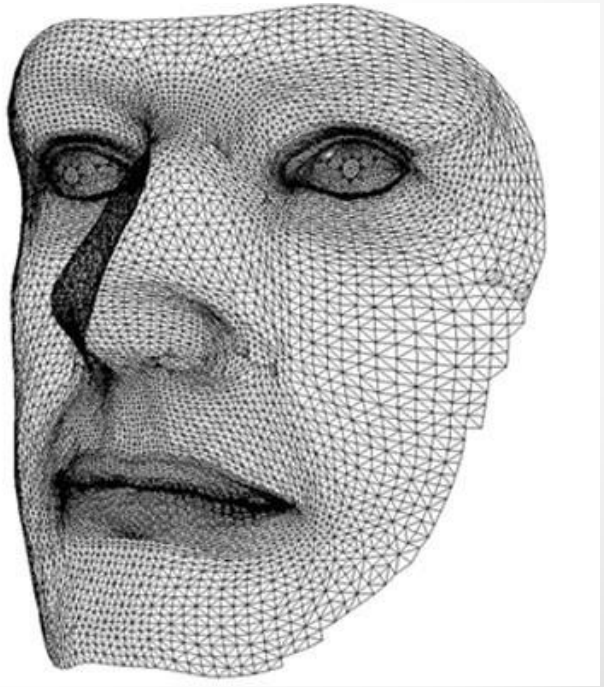
Биометрия



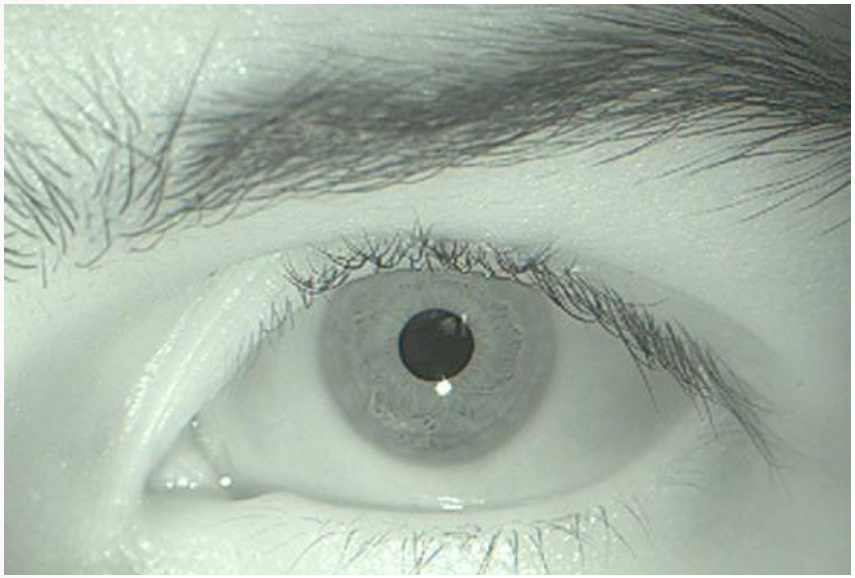
Биометрия

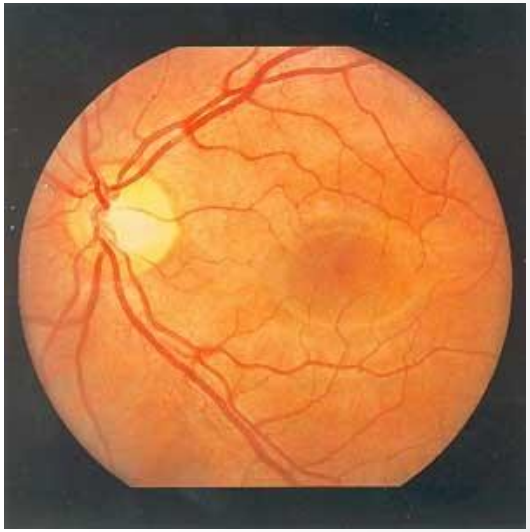
Биометрия





Биометрия





Биометрия

Комбинированные средства

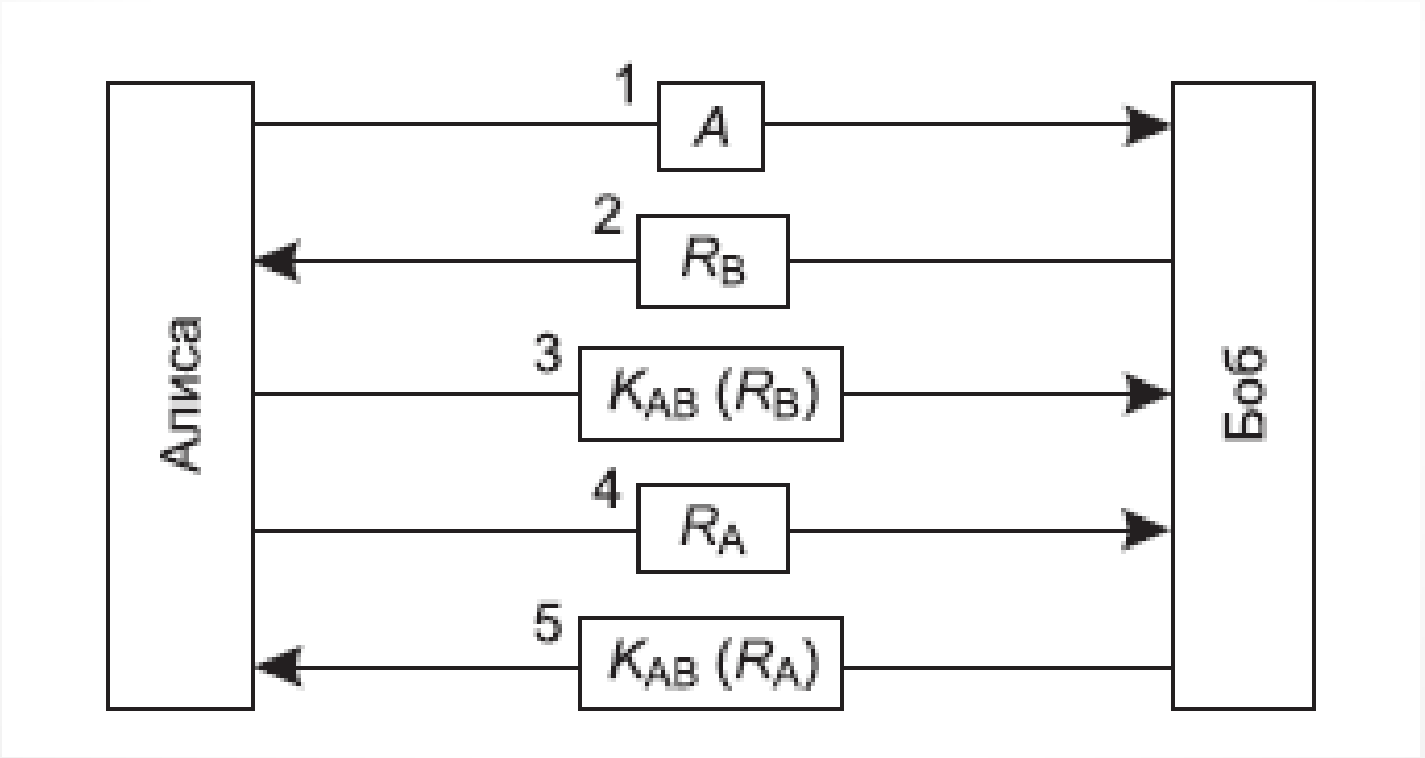
Протоколы удаленной аутентификации

Условные обозначения:

- *A* и *B* — Алиса и Боб;
- R_i — оклик, где индекс означает его отправителя;
- K_i — ключи, где индекс означает владельца ключа;
- K_S — ключ сеанса.

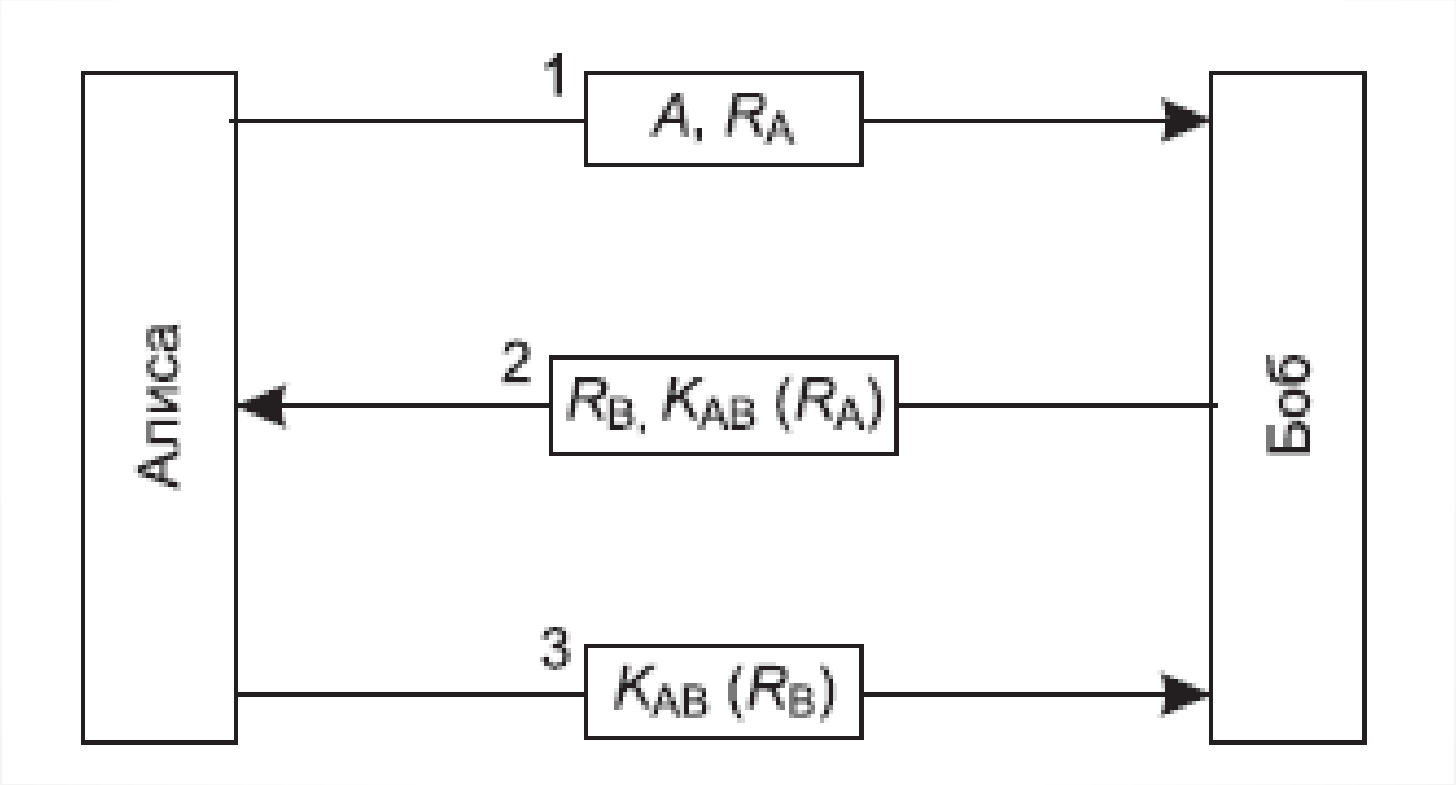
Протоколы удаленной аутентификации

Двусторонняя аутентификация при помощи протокола **«оклик – отзыв»**



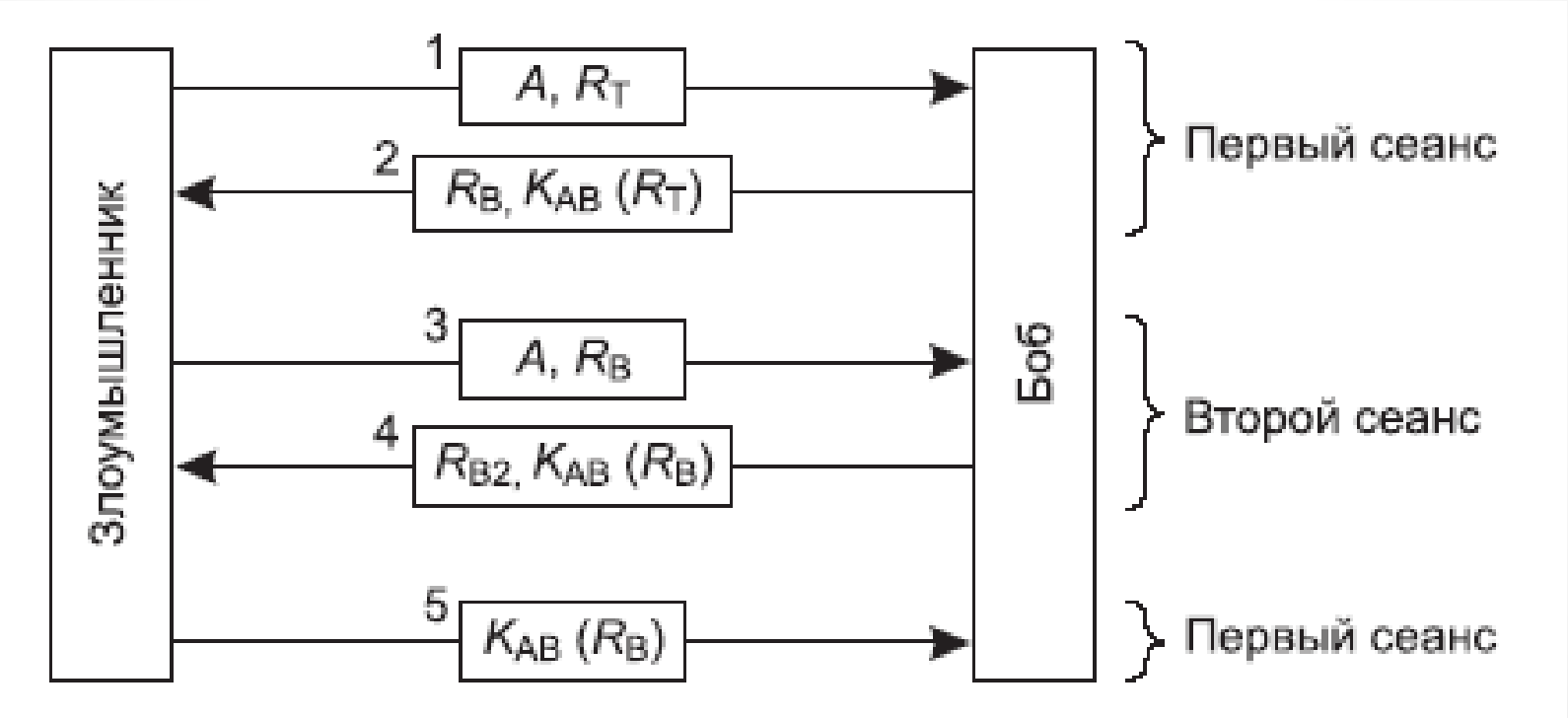
Протоколы удаленной аутентификации

Укороченный двусторонний протокол аутентификации

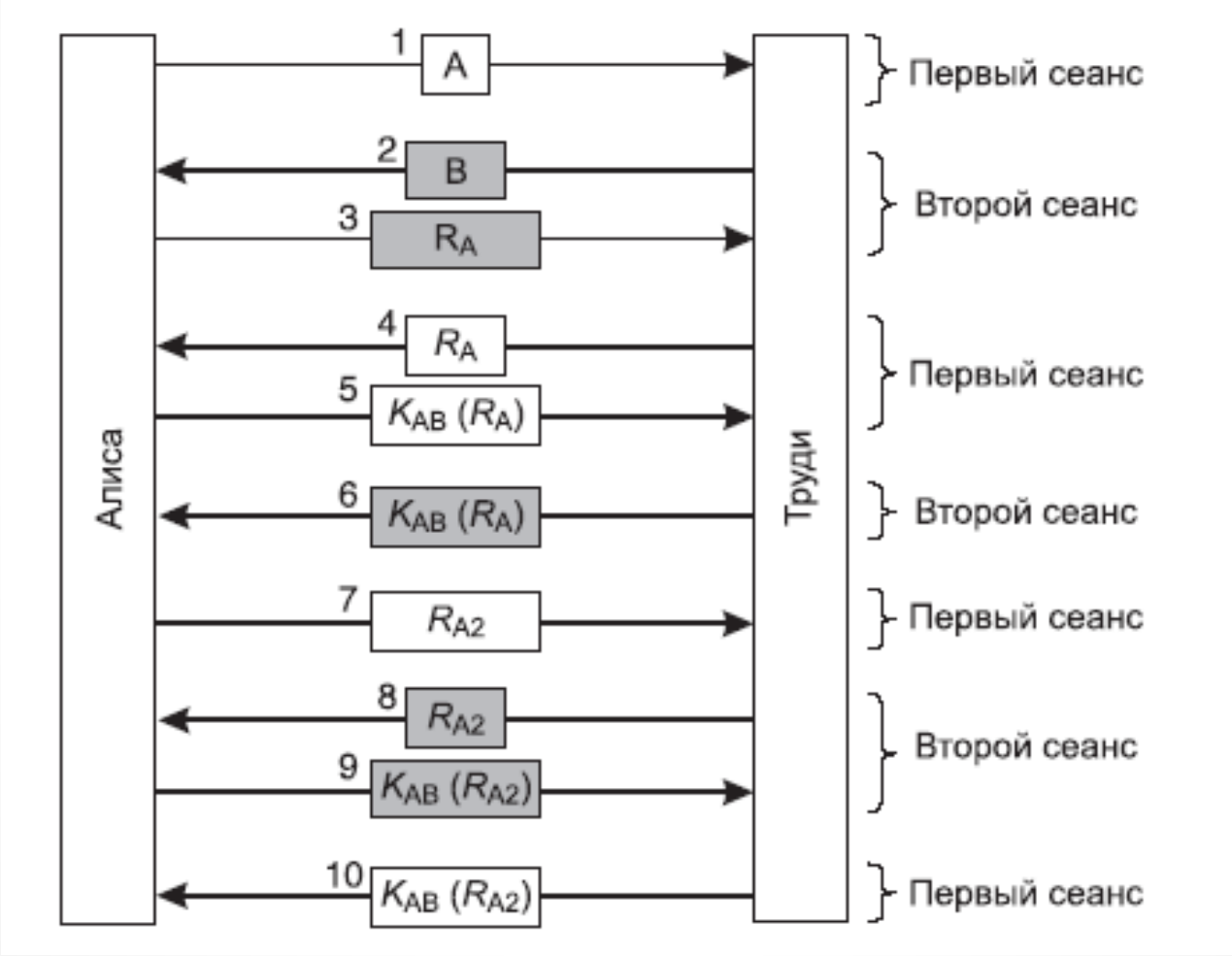


Протоколы удаленной аутентификации

Зеркальная атака



Протоколы удаленной аутентификации



Протоколы удаленной аутентификации

Общие правила разработки протокола аутентификации:

1. Инициатор сеанса должен подтверждать свою личность прежде, чем это сделает отвечающая сторона. Это помешает злоумышленнику получить ценную для него информацию, прежде чем он подтвердит свою личность.

2. Следует использовать два раздельных общих секретных ключа: один для инициатора сеанса, а другой для отвечающего, K_{AB} и K'_{AB}.

Протоколы удаленной аутентификации

Общие правила разработки протокола аутентификации (окончание):

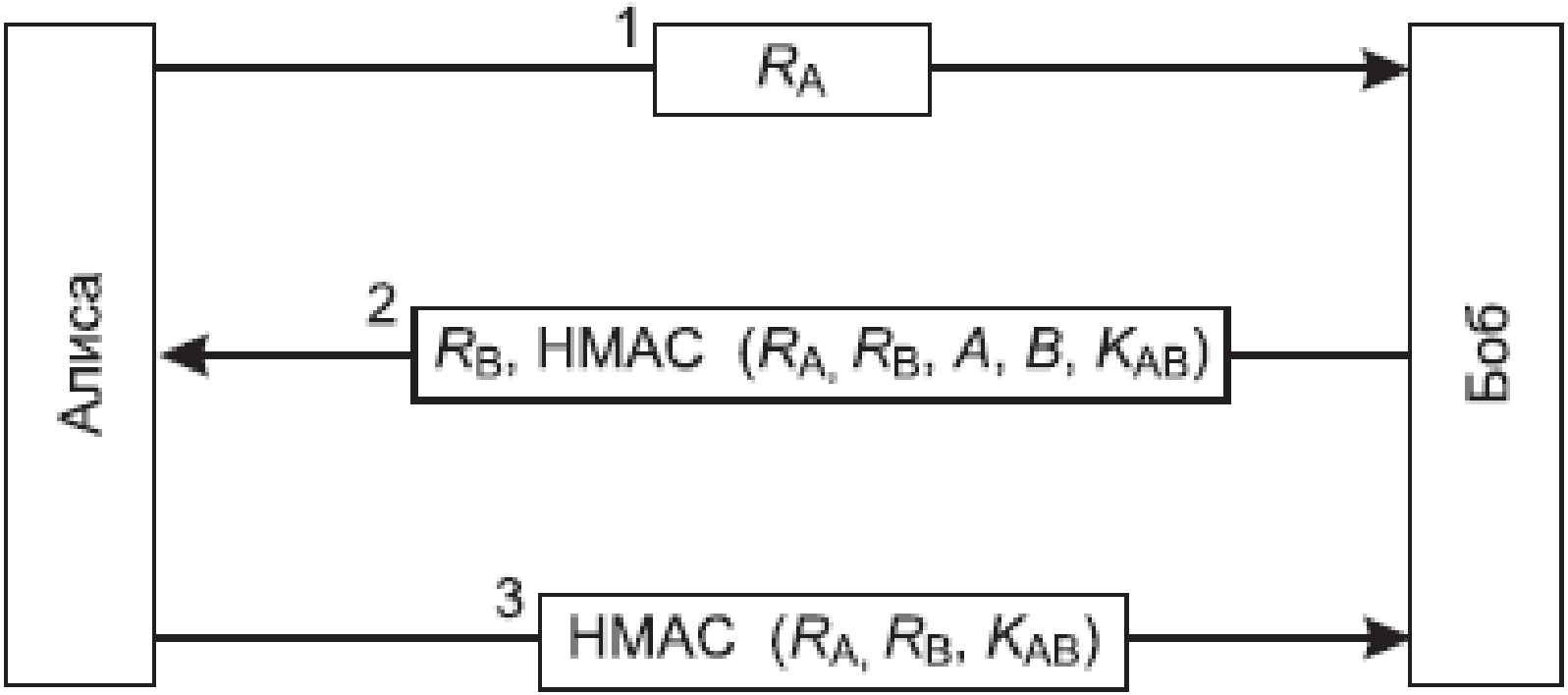
3. Инициатор и отвечающий должны выбирать оклики из различных непересекающихся наборов. Например, инициатор должен пользоваться четными номерами, а отвечающий — нечетными.

4. Протокол должен уметь противостоять атакам, при которых запускается второй параллельный сеанс, информация для которого извлекается при помощи первого сеанса (или наоборот).

Если нарушается хотя бы одно из этих правил, протокол оказывается уязвимым.

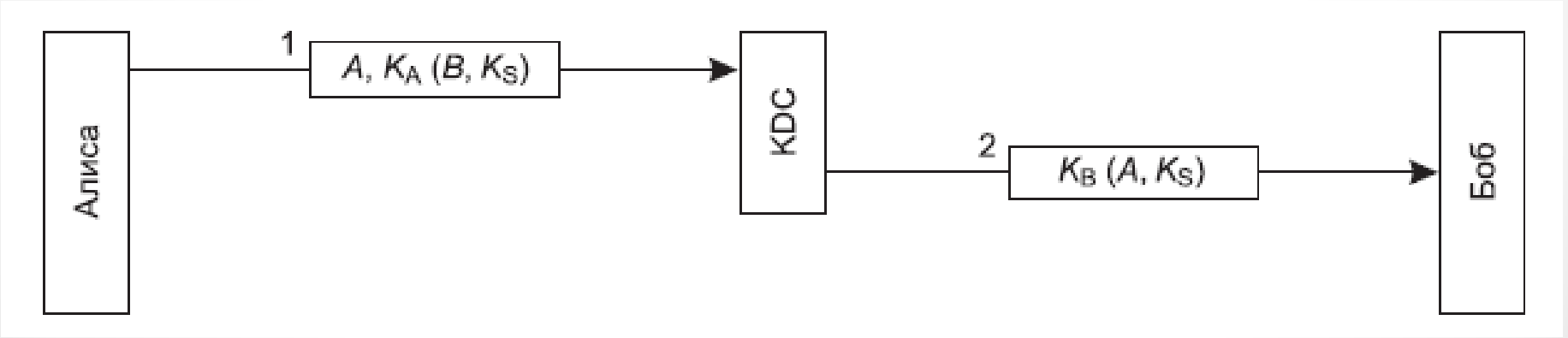
Протоколы удаленной аутентификации

Аутентификация с применением хэш-кода



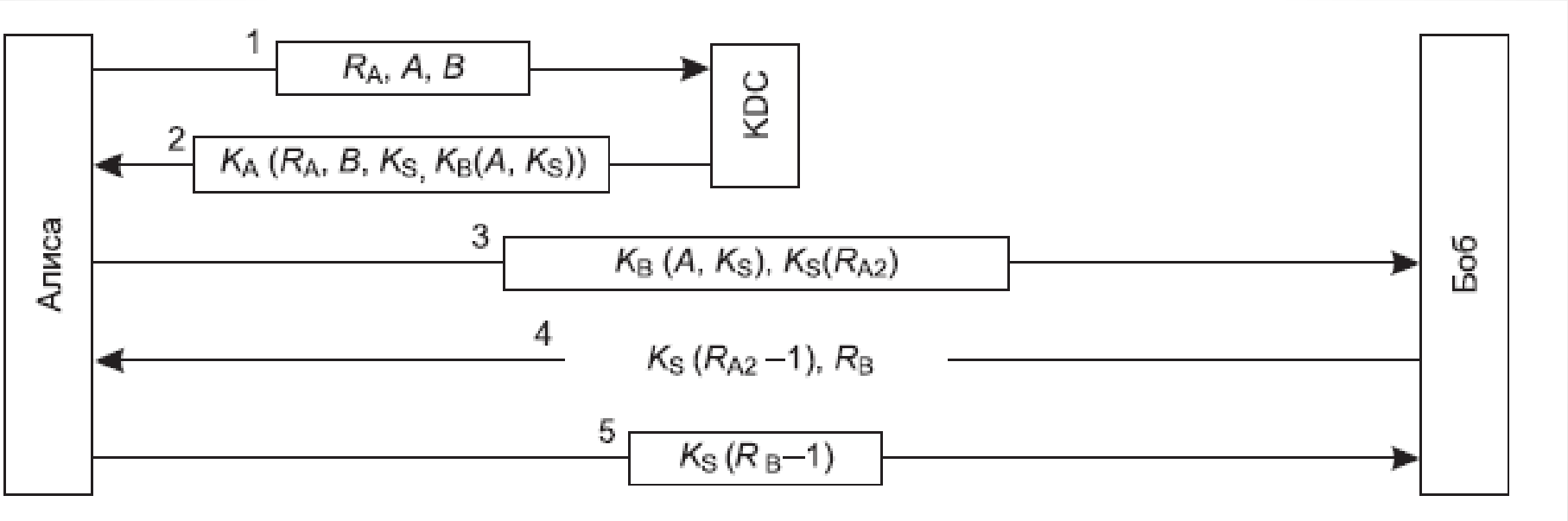
Протоколы удаленной аутентификации

Аутентификация с помощью центра распространения ключей



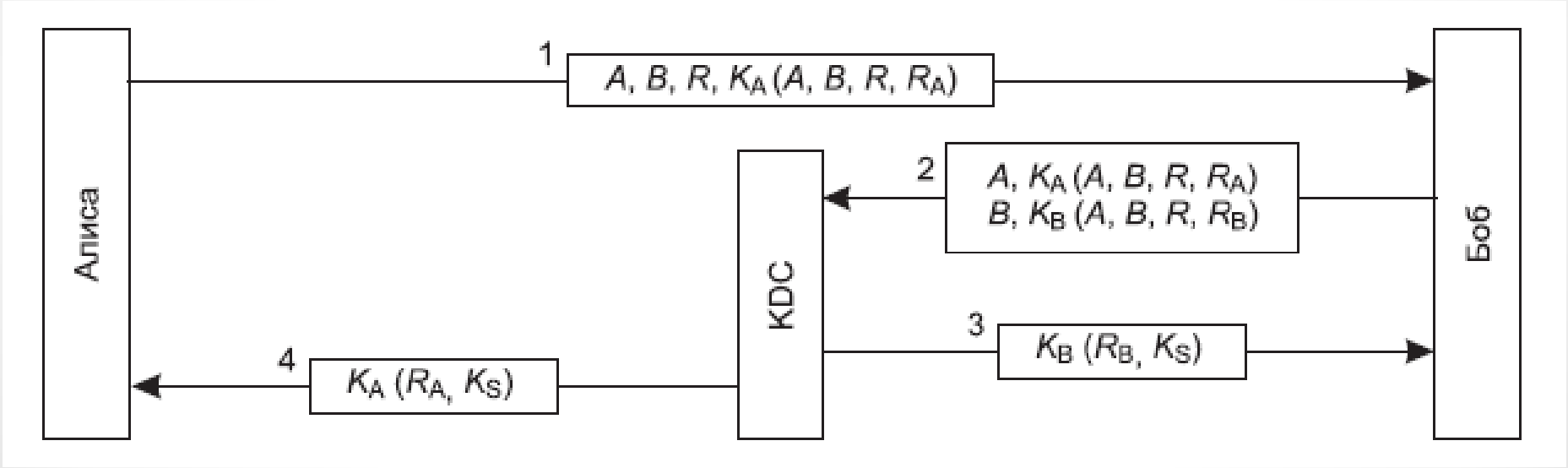
Протоколы удаленной аутентификации

Протокол аутентификации Нидхэма-Шредера



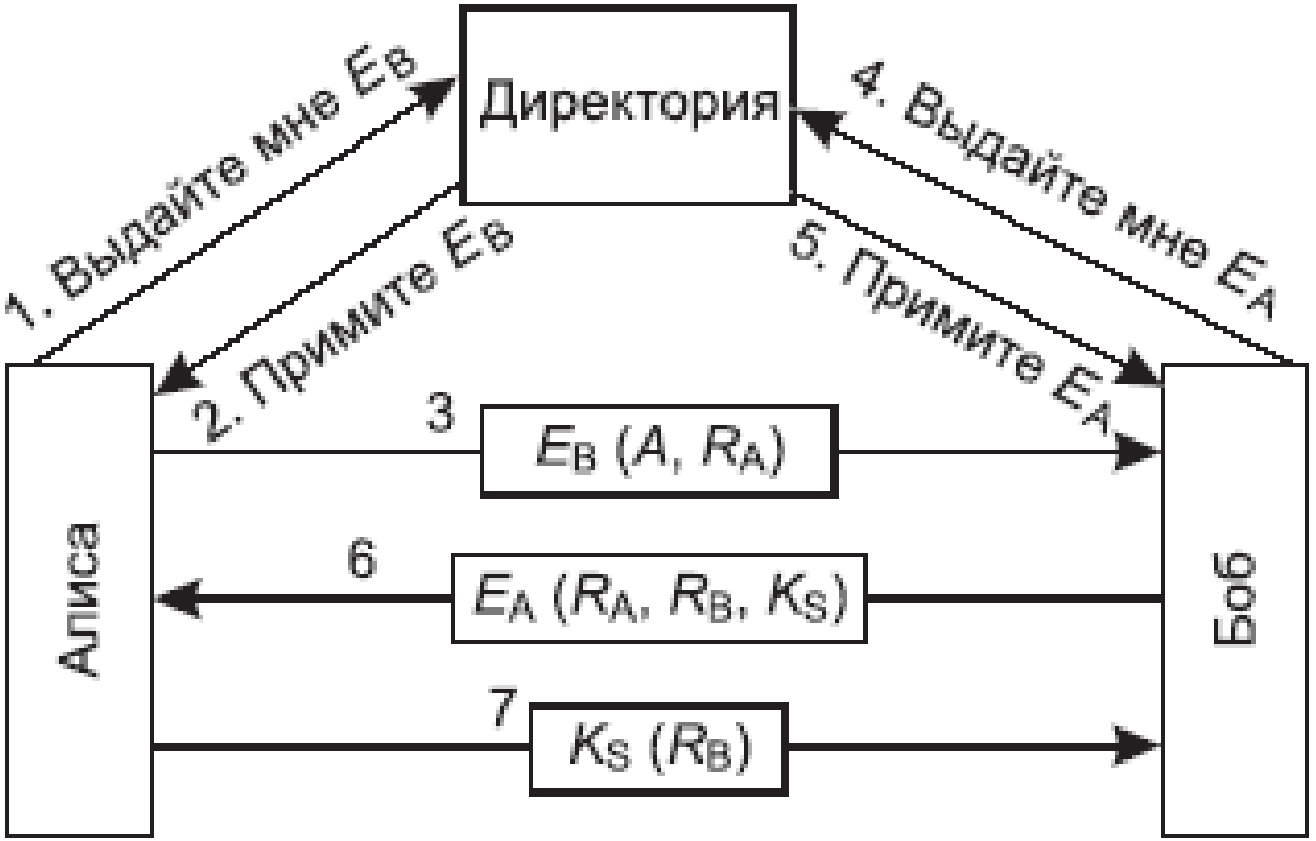
Протоколы удаленной аутентификации

Протокол аутентификации Отуэя-Риса



Протоколы удаленной аутентификации

Взаимная аутентификация с помощью открытого ключа



Управление доступом в операционных системах

В работе протокола **Kerberos**, помимо рабочей (клиентской) станции Алисы, принимают участие еще три сервера:

1. **Сервер аутентификации** (**AS**, **Authentication Server**): проверяет личность пользователей при входе в сеть.

2. **Сервер выдачи билетов** (**TGS**, **Ticket Granting Server**): выдает «билеты, подтверждающие подлинность».

3. **Боб**, то есть сервер, предоставляющий услуги Алисе.

Управление доступом в операционных системах

Работа протокола Kerberos v5