# Тема 12

Средства аутентификации субъектов и управление доступом

# Содержание темы

- Понятие идентификации и аутентификации.
- Классификация средств аутентификации.
- Парольные средства аутентификации для оконечных устройств телекоммуникационных систем.
- Средства аутентификации с использованием смарт-карт и электронных ключей.
- Биометрические средства аутентификации.

# Содержание темы

- Строгая аутентификация в компьютерных сетях.
- Протоколы аутентификации.
- Технологии управления доступом и авторизация.
- Дискретный и мандатный методы управления доступом.
- Ролевое управление доступом.
- Управление доступом в операционных системах.

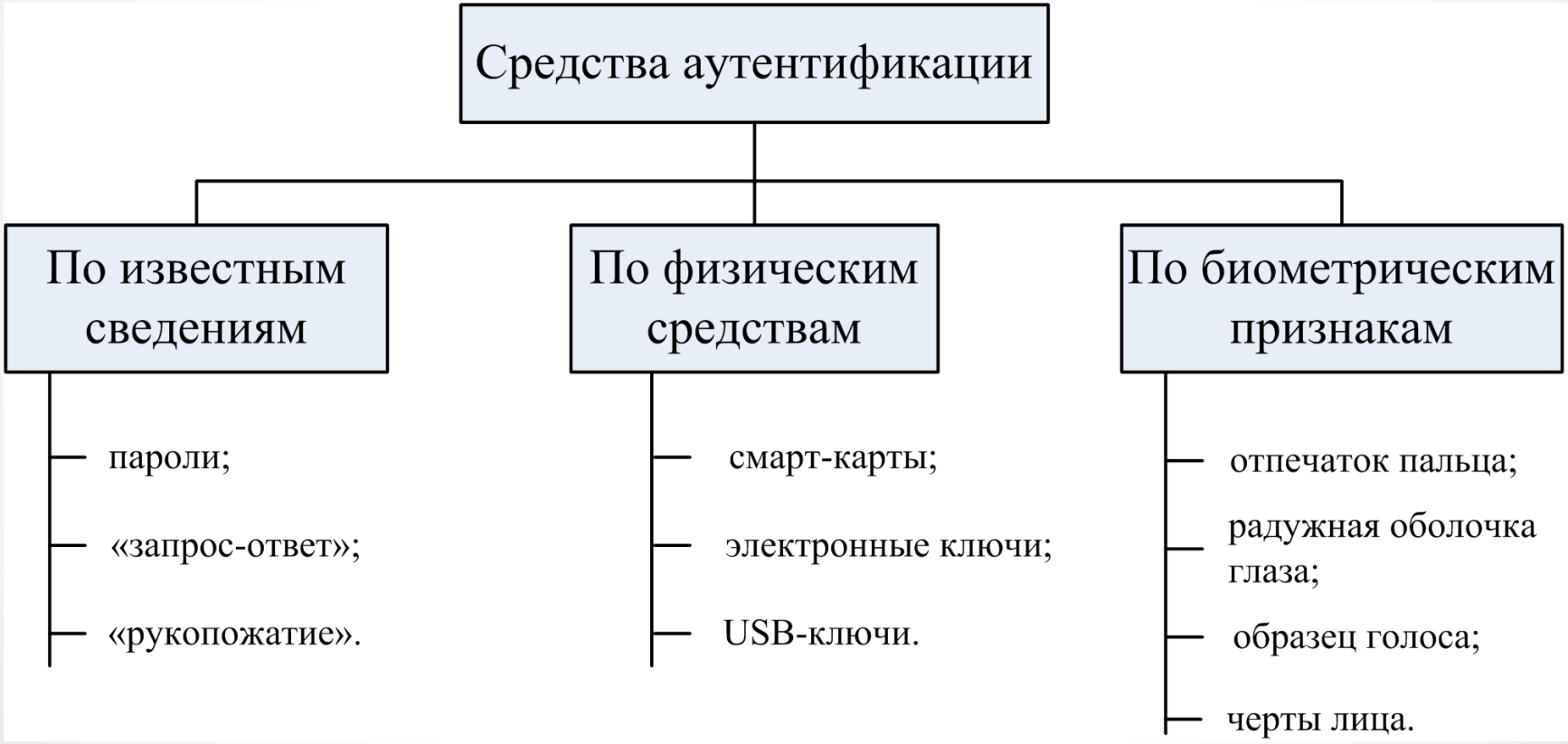
# Идентификация и аутентификация

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

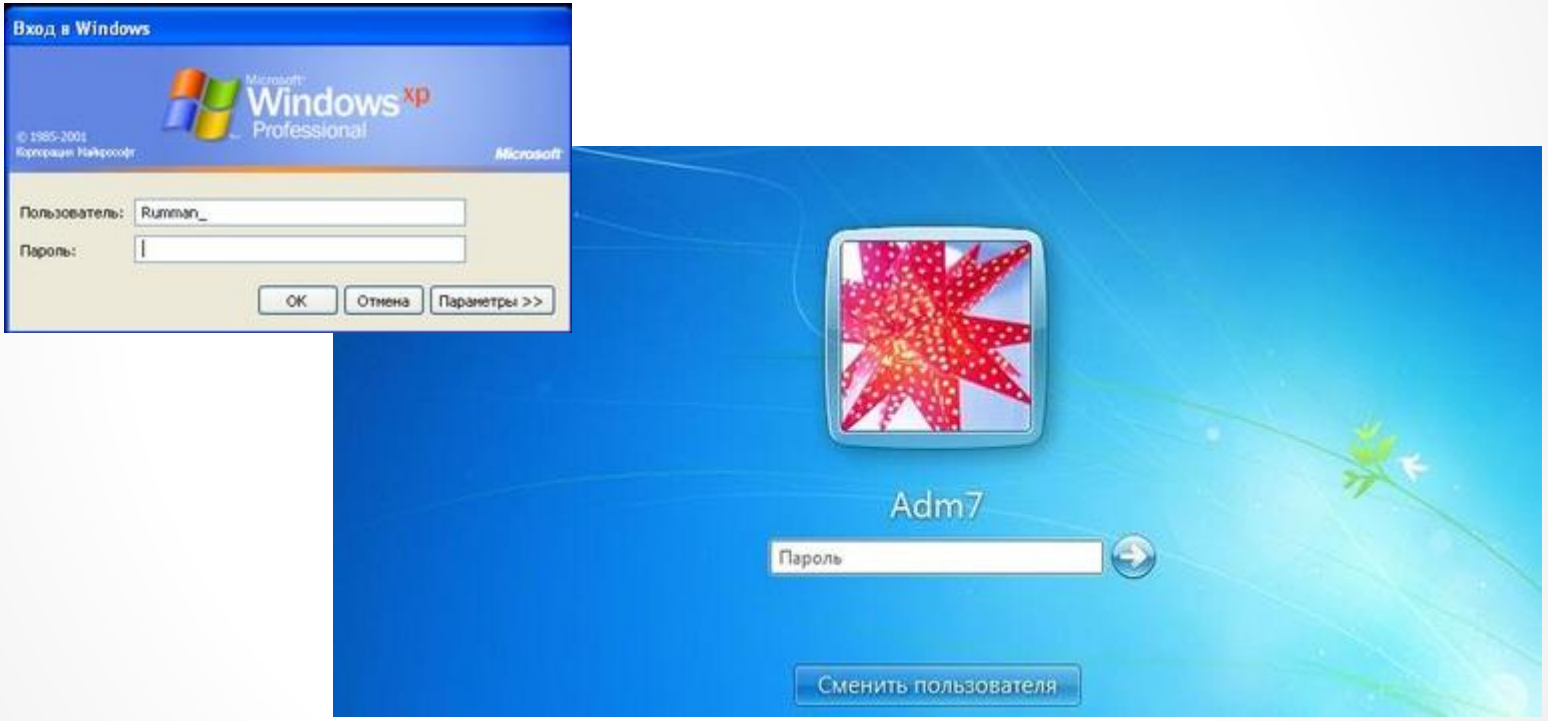
**Аутентификация** – это процесс, который обеспечивает проверку законности субъекта аутентификации и устанавливает, является ли он тем, за кого себя выдает.

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

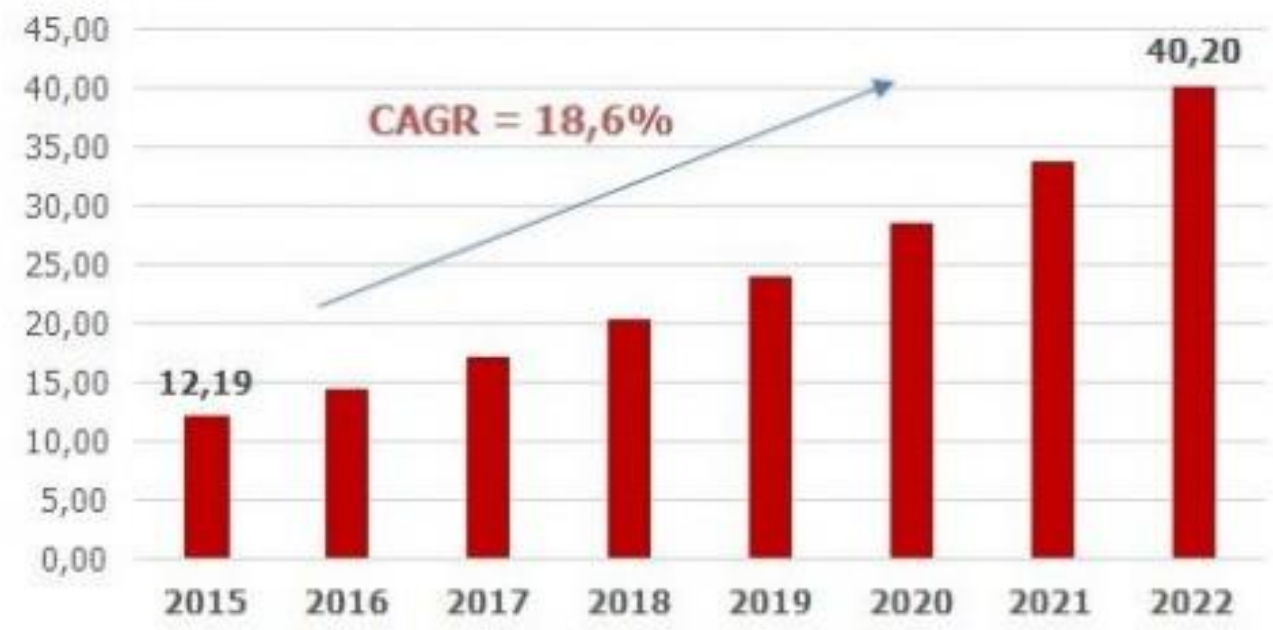
Электронный ключ (iButton)
48-битный код


Смарт-карта
код от 64 бит

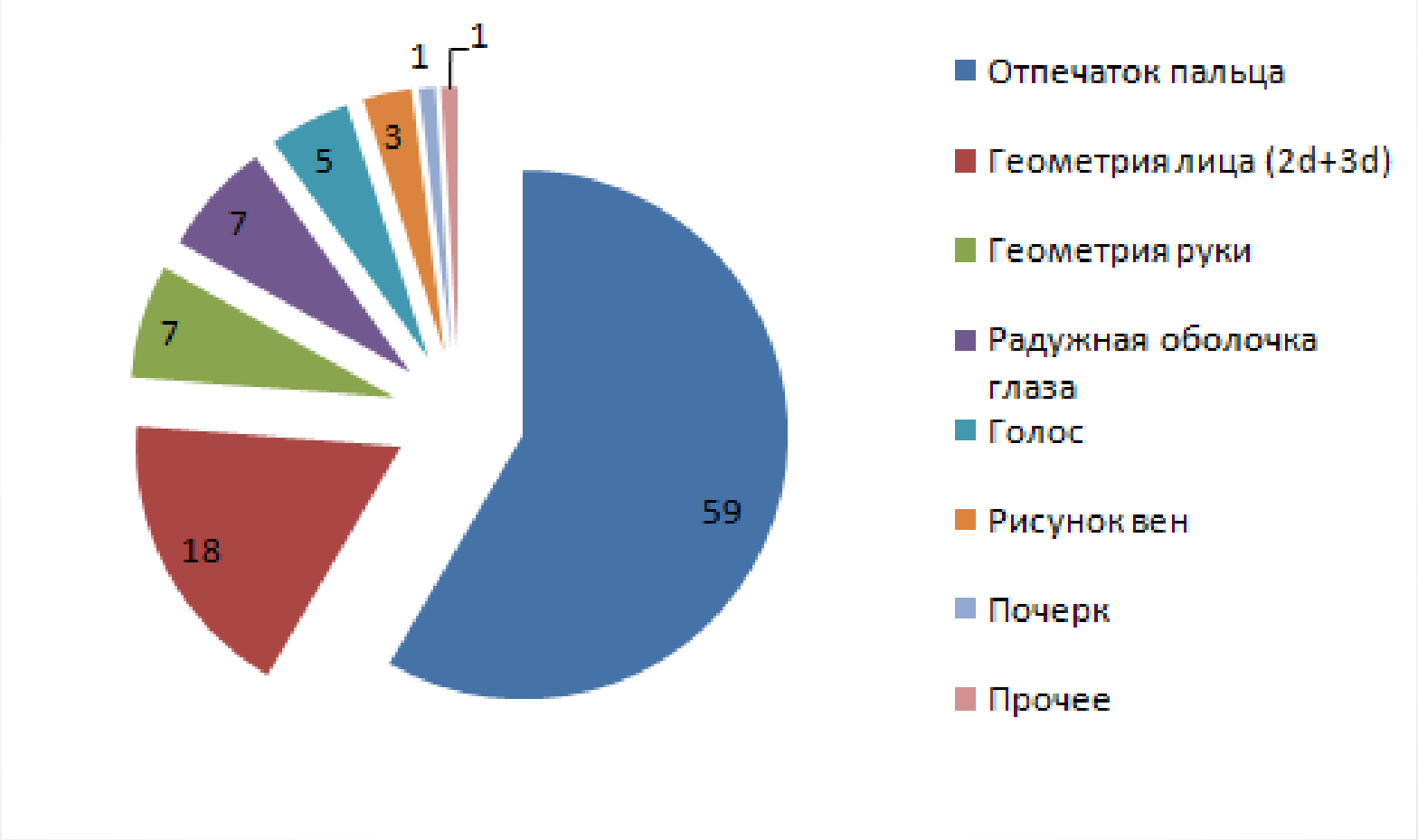
USB-ключ

# Биометрия

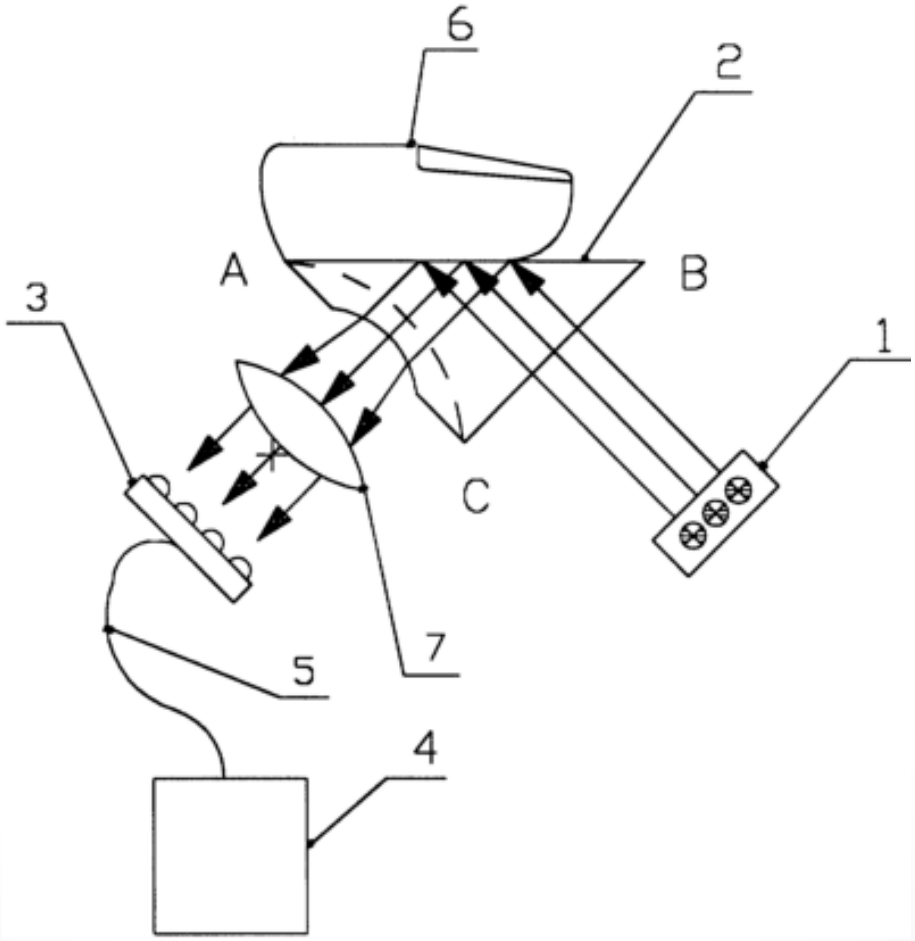
Рис. 1. Объем мирового рынка биометрических систем в 2015-2022 гг., $млрд.



# 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

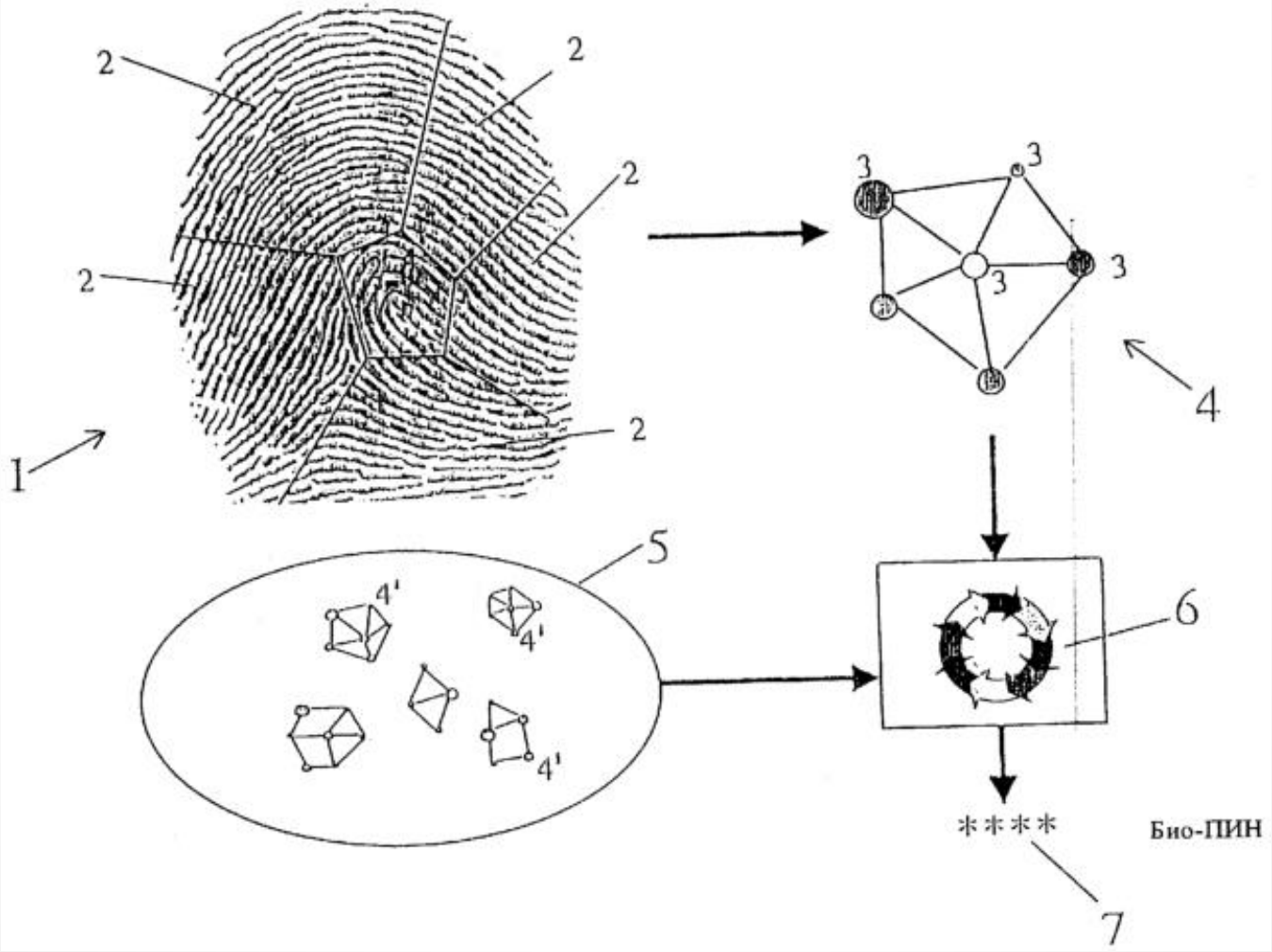


# Биометрия


**Папиллярные линии** – рельефные линии на ладонных и подошвенных поверхностях.

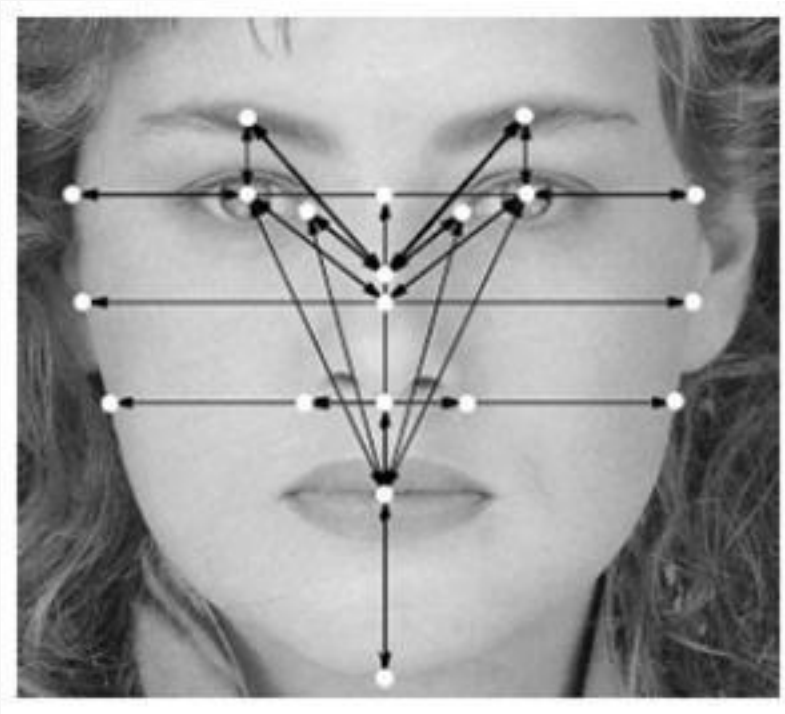
**Минуции** – участки папиллярного рисунка кожи, где отдельные линии сливаются, раздваиваются или обрываются.

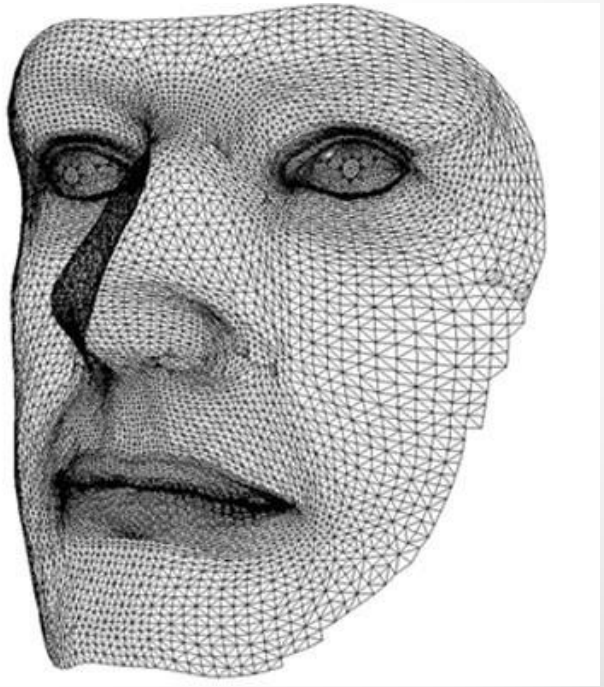
# Биометрия



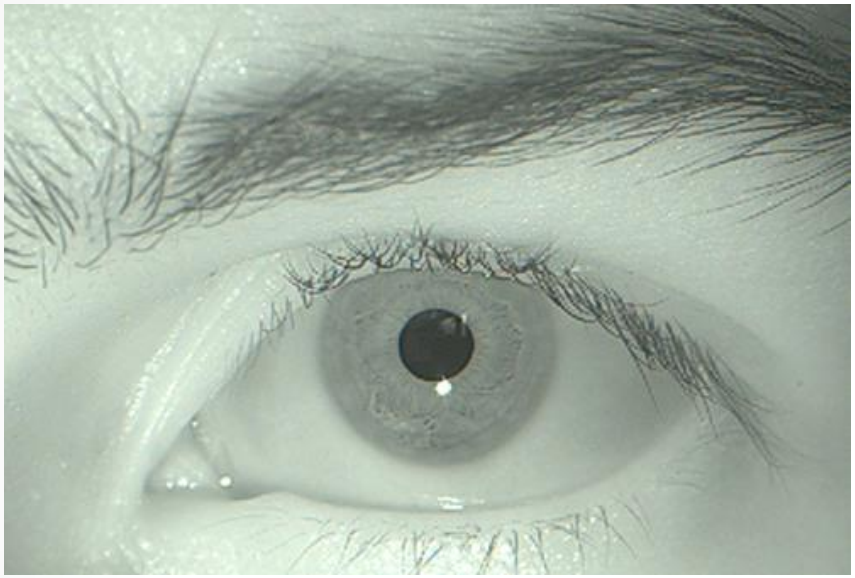
# Биометрия

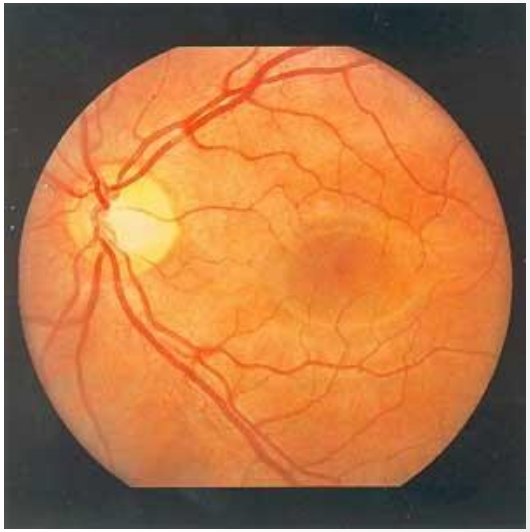
# Биометрия





# Биометрия





# Биометрия

# Комбинированные средства

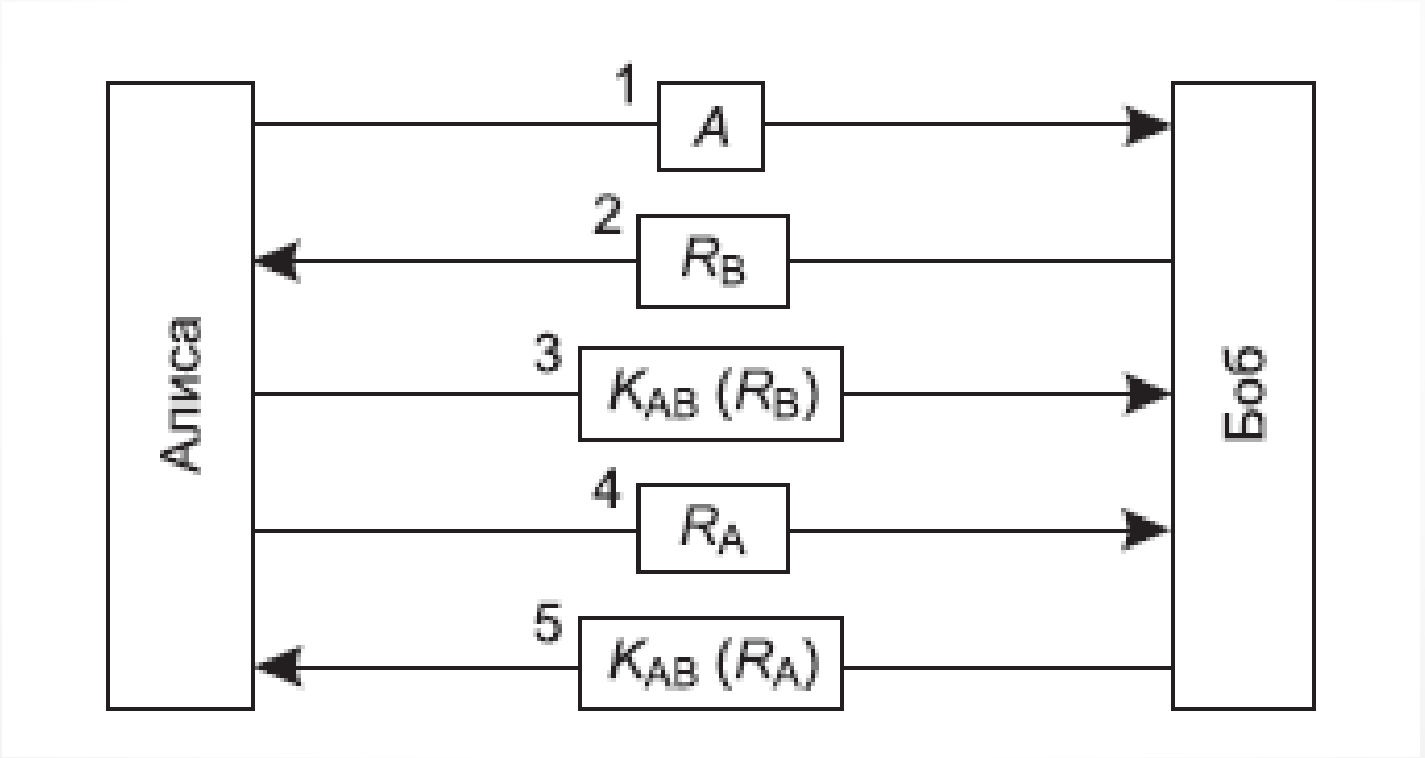
# Протоколы удаленной аутентификации

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.

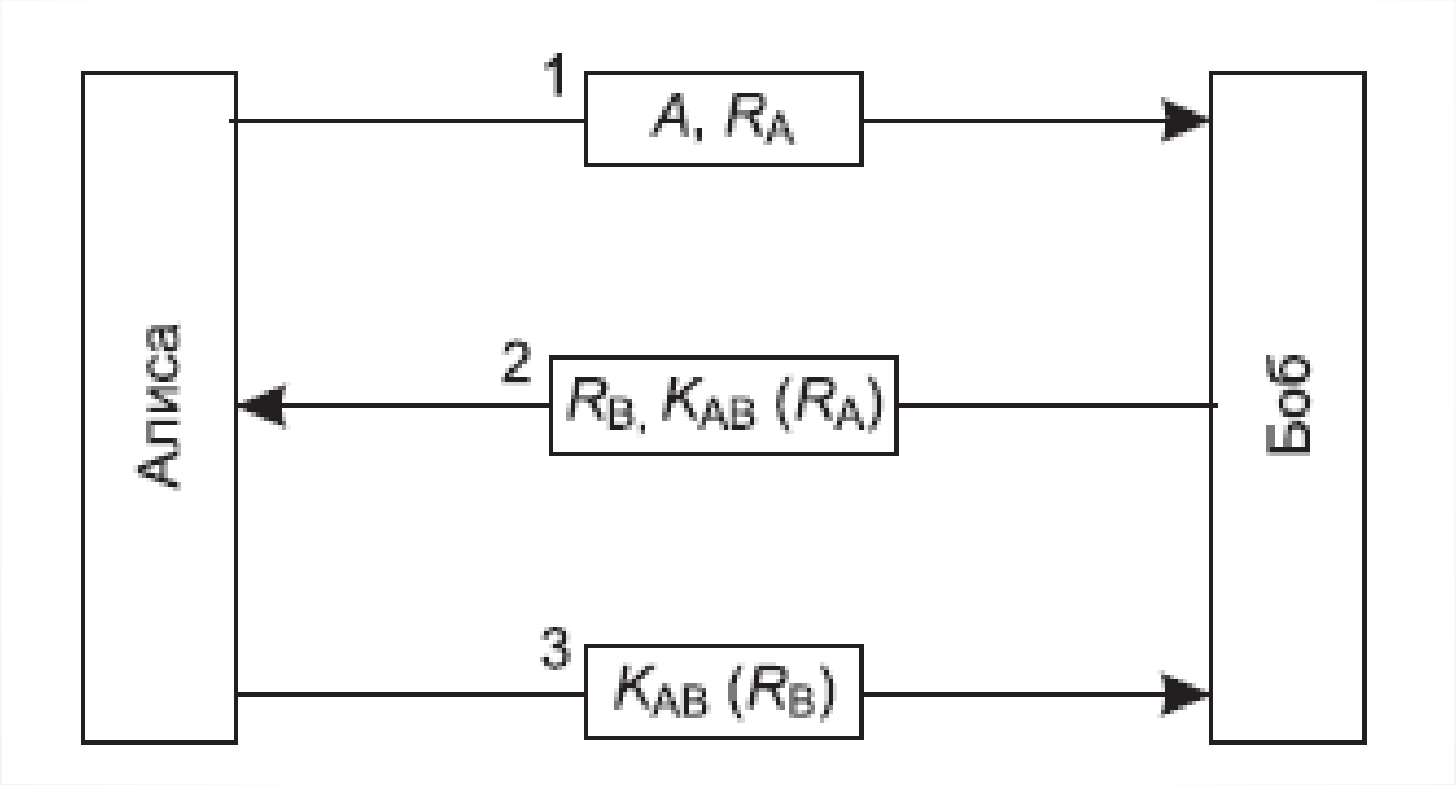
# Протоколы удаленной аутентификации

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



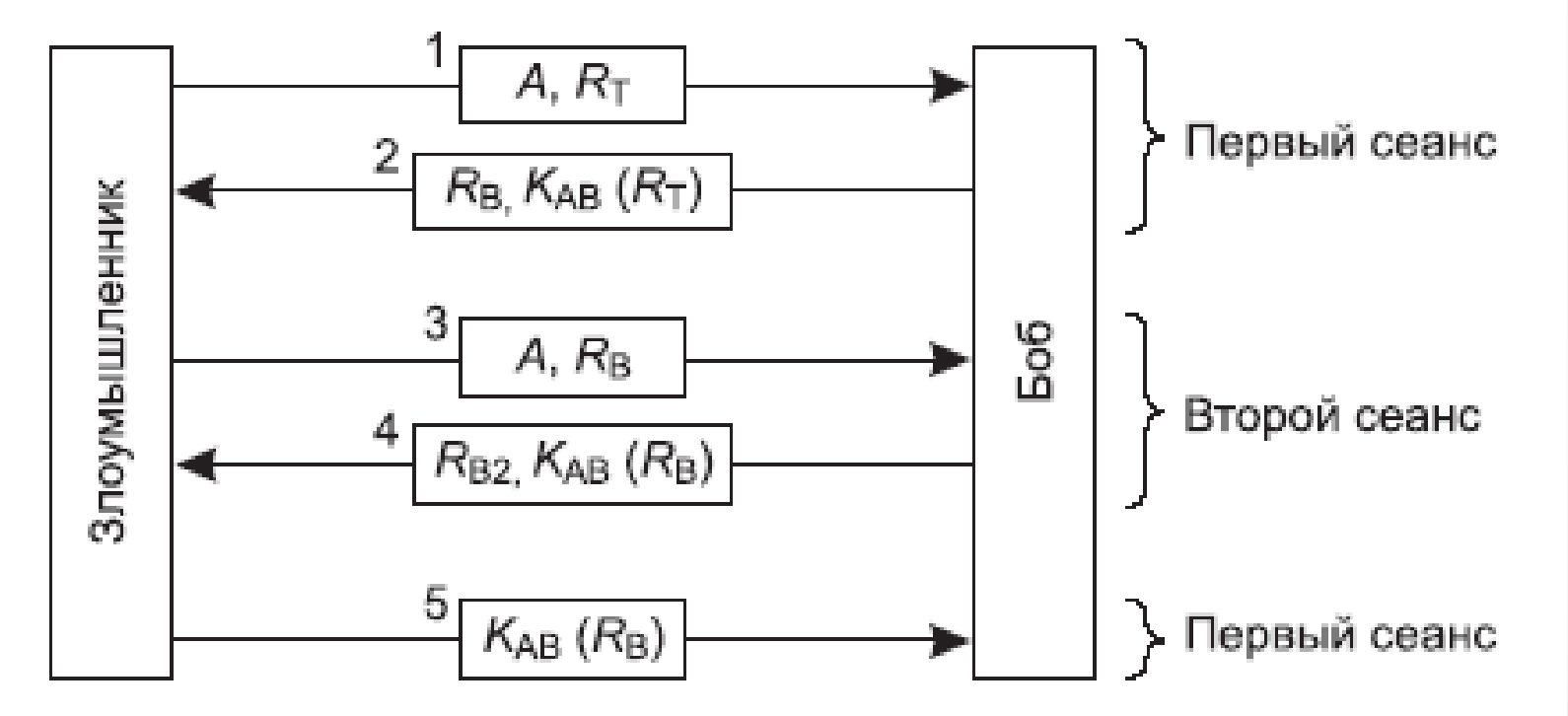
# Протоколы удаленной аутентификации

**Укороченный двусторонний протокол аутентификации**

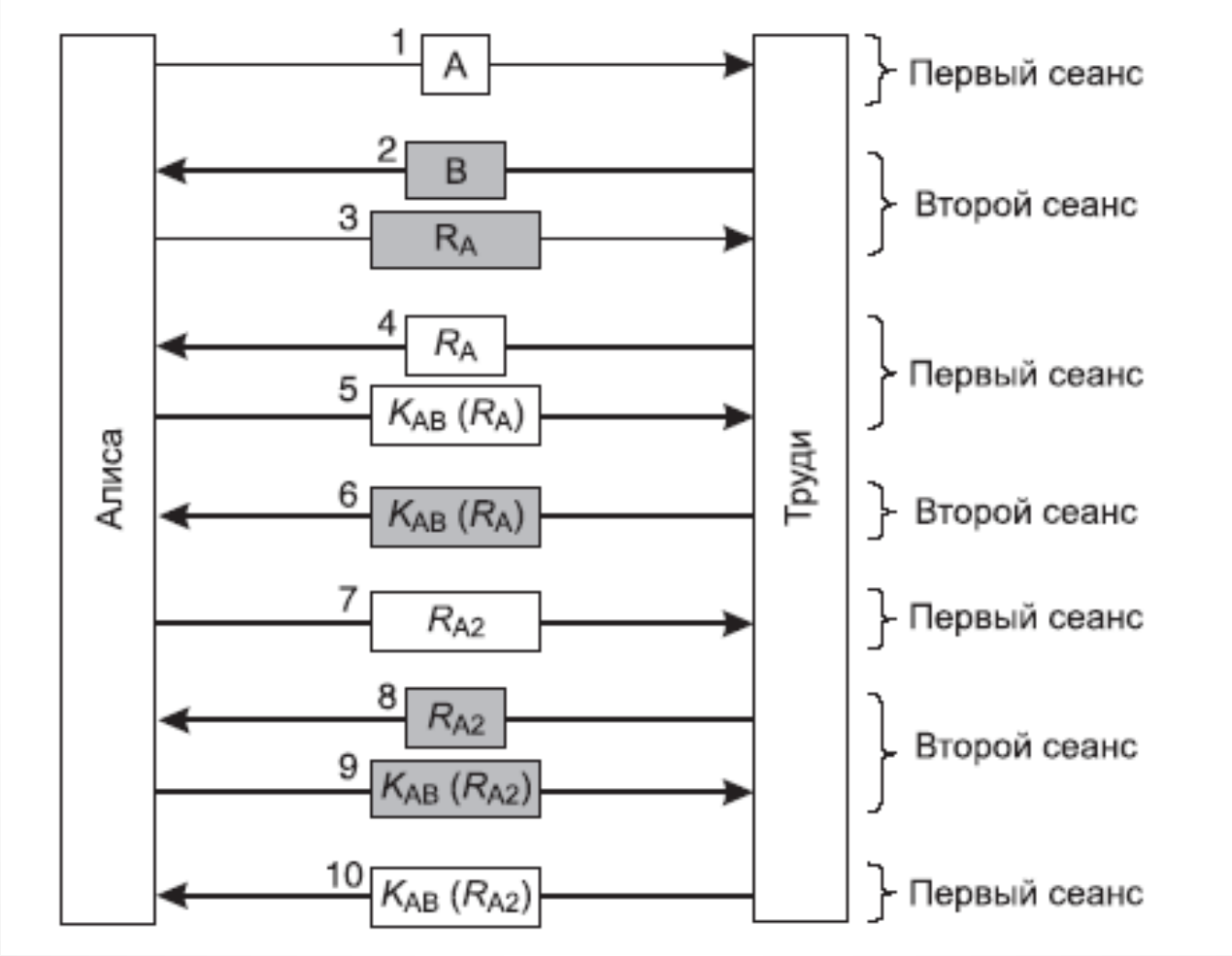


# Протоколы удаленной аутентификации

## 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):**

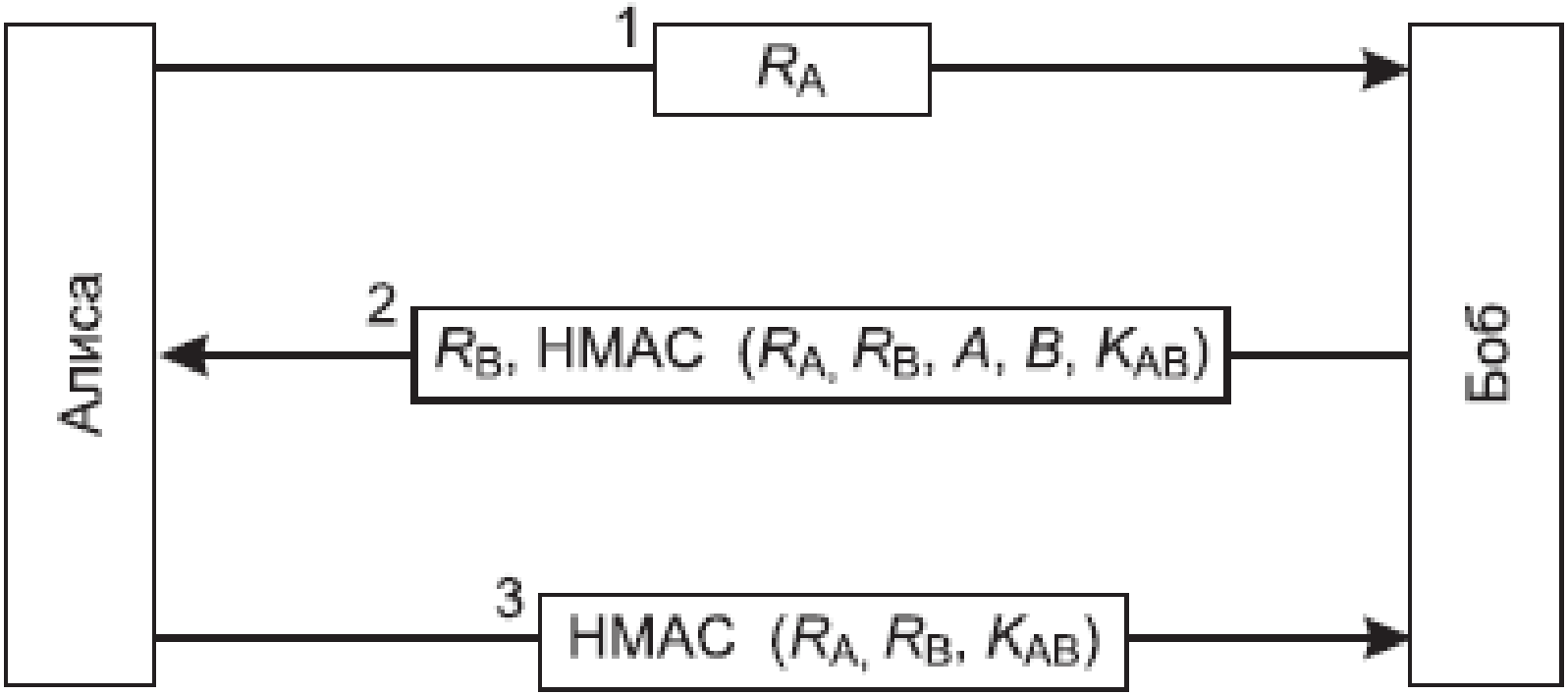
3. Инициатор и отвечающий должны выбирать оклики из различных непересекающихся наборов. Например, инициатор должен пользоваться четными номерами, а отвечающий — нечетными.

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.

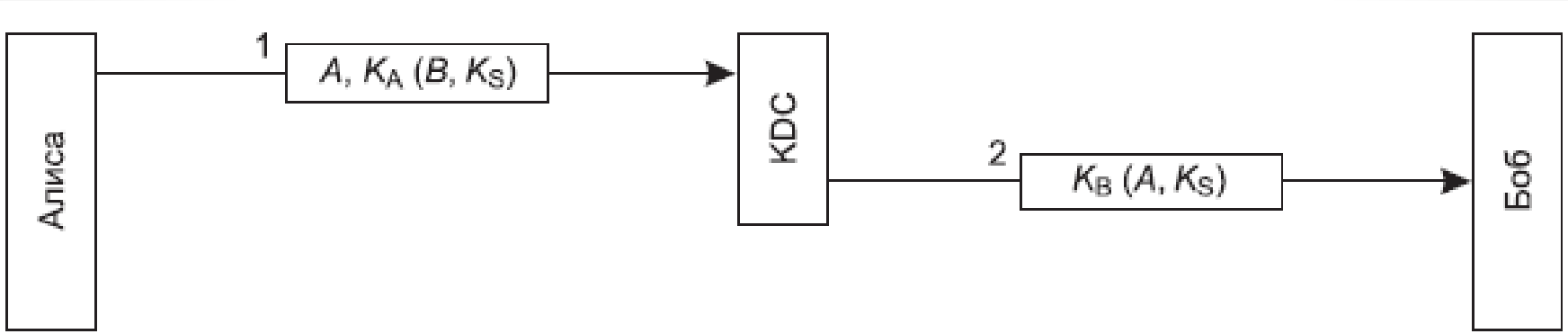
# Протоколы удаленной аутентификации

## Аутентификация с применением хэш-кода



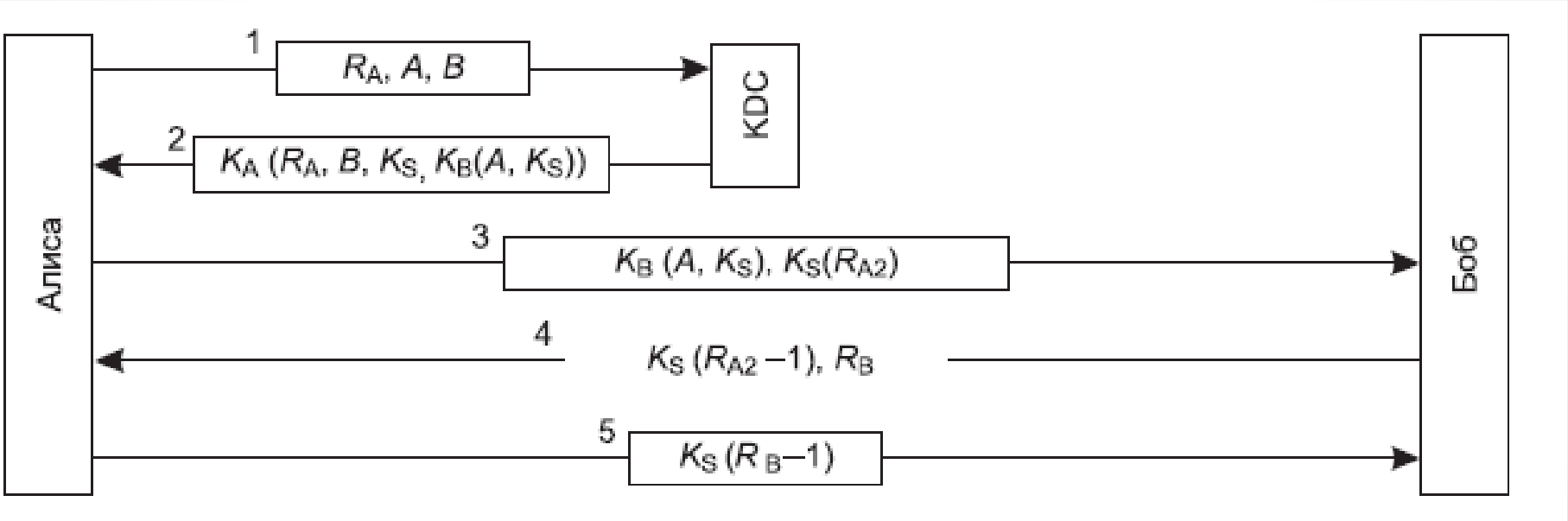
# Протоколы удаленной аутентификации

**Аутентификация с помощью центра распространения ключей**



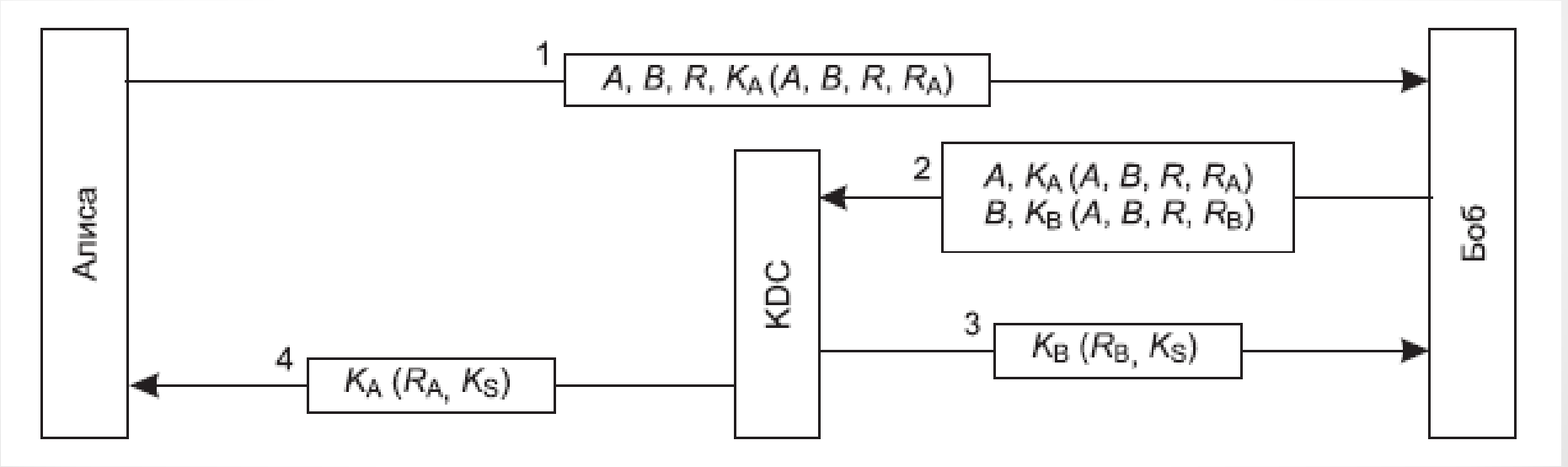
# Протоколы удаленной аутентификации

## Протокол аутентификации Нидхэма-Шредера



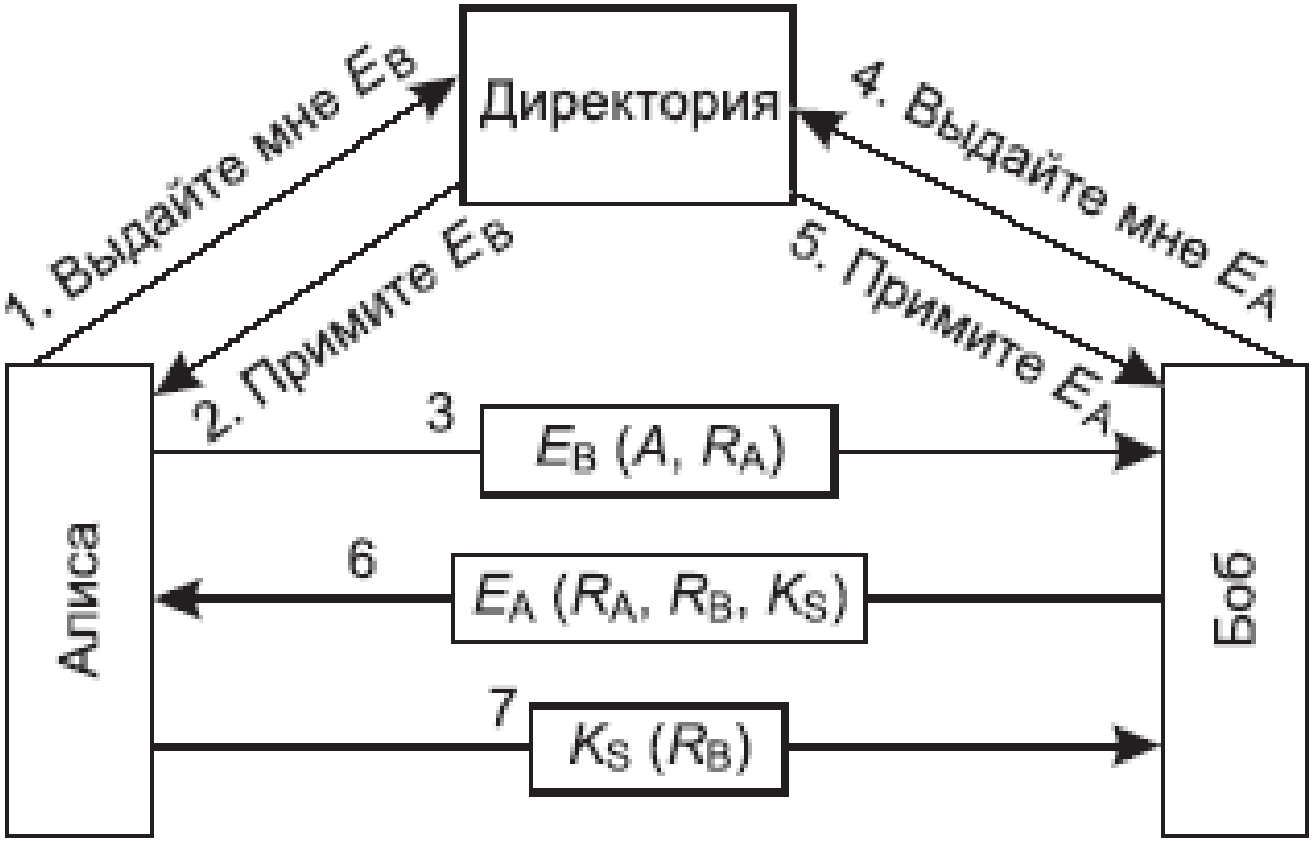
# Протоколы удаленной аутентификации

## Протокол аутентификации Отуэя-Риса



# Протоколы удаленной аутентификации

**Взаимная аутентификация с помощью открытого ключа**



# Авторизация субъектов

**Авторизация** - это процедура контроля доступа легальных субъектов к ресурсам системы и предоставление каждому из них именно тех прав, которые ему были определены администратором.

Термин **авторизация** (authorization) происходит от латинского слова auctoritas, показывающее уровень престижа человека в Древнем Риме и соответствующие этому уровню привилегии.

Помимо предоставления пользователям прав доступа к каталогам, файлам и принтерам, средства авторизации могут контролировать возможность выполнения пользователями различных системных функций.

# Принципы организации разграничения доступа

Ограничение доступа может задаваться в форме **правил**.

На основании правил система управления доступом в любой момент времени динамически решает вопрос о предоставлении или не предоставлении доступа.

Правило строится с учетом различных факторов, например:

- длительность сеанса связи;
- возраст;
- время суток и т. п.

# Принципы организации разграничения доступа

Разграничение доступа может осуществляться несколькими способами:

- По **спискам контроля доступа** (**ACL – Access Control List**);
- С использованием **избирательного** или **дискреционного управления доступом** (**DAC – Discretionary Access Control**, матрицей контроля доступа);
- С помощью **полномочного** или **мандатного управления доступом** (**MAC – Mandatory Access Control**) – по уровням секретности;
- По **ролевому доступу** (**RBAC – Role-based Access Control**) – недискреционному методу доступа.

# Принципы организации разграничения доступа

Разграничение доступа по **спискам контроля доступа** заключается в том, что для каждого элемента защищаемых данных (файла, базы, программы) составляется список всех тех пользователей, которым предоставлено право доступа к соответствующему элементу, или, наоборот, для каждого зарегистрированного пользователя составляется список тех элементов защищаемых данных, к которым ему предоставлено право доступа.

# Принципы организации разграничения доступа

**Избирательное** или **дискреционное управление доступом** (разграничение доступа по матрицам полномочий) предполагает формирование двумерной матрицы, по строкам которой содержатся идентификаторы зарегистрированных пользователей, а по столбцам – идентификаторы защищаемых элементов данных (*X* – нет прав; *R* – чтение; *W* – запись; *C* – создание; *E* – редактирование; *D* – удаление).

| Субъект | Объект | | | |
|---|---|---|---|---|
| | персональные данные сотрудника | финансовый отчет | методическое пособие | приказ |
| **Ректор** | R | R | R | R, W, C, D |
| **Главный бухгалтер** | R | W, C, E | R | R |
| **Преподаватель** | X | X | W, R, C, E, D | R |
| **Студент** | X | X | R | R |

# Принципы организации разграничения доступа

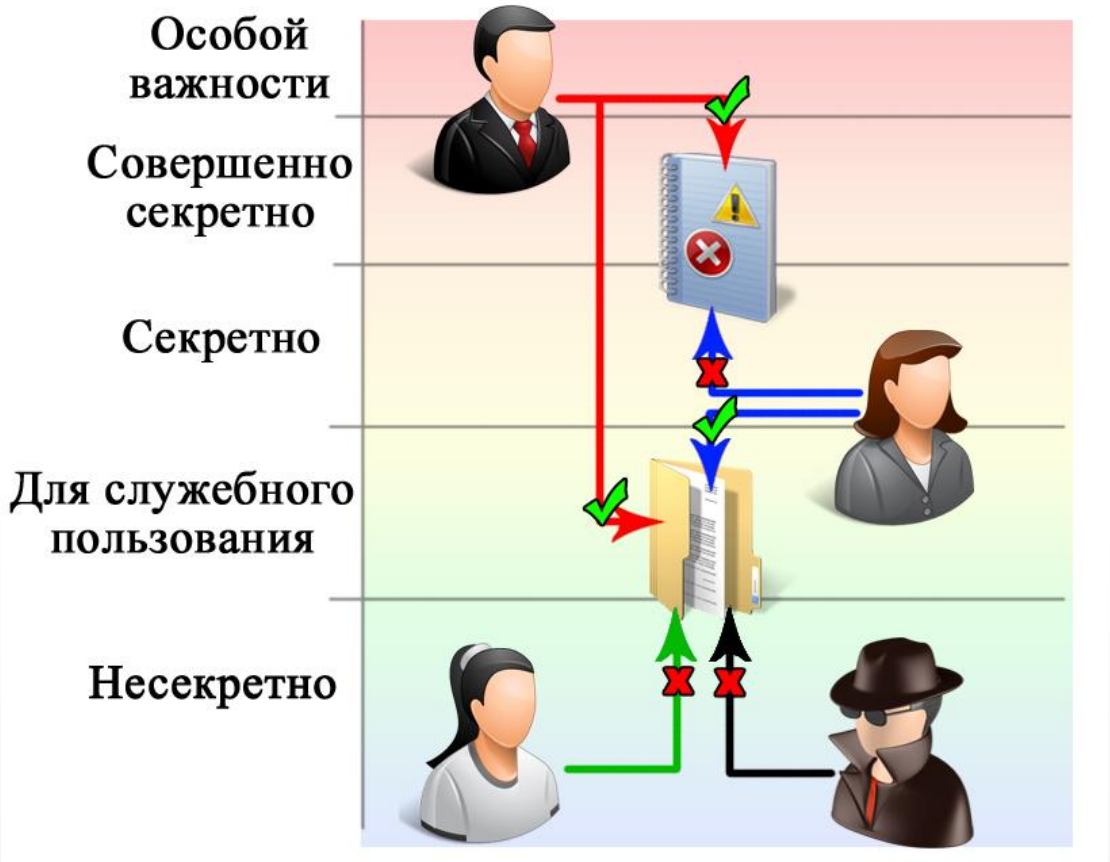
Схема реализации дискреционного управления доступом

# Принципы организации разграничения доступа

**Полномочное** (**мандатное**) **управление доступом** есть способ разового разрешения на допуск к защищаемому элементу данных. Заключается он в том, что каждому защищаемому элементу присваивается персональная уникальная метка, после чего доступ к этому элементу будет разрешен только тому пользователю, который в своем запросе предъявит метку элемента (мандат), которую ему может выдать администратор защиты или владелец элемента.

# Принципы организации разграничения доступа

Схема реализации мандатного управления доступом



# Принципы организации разграничения доступа

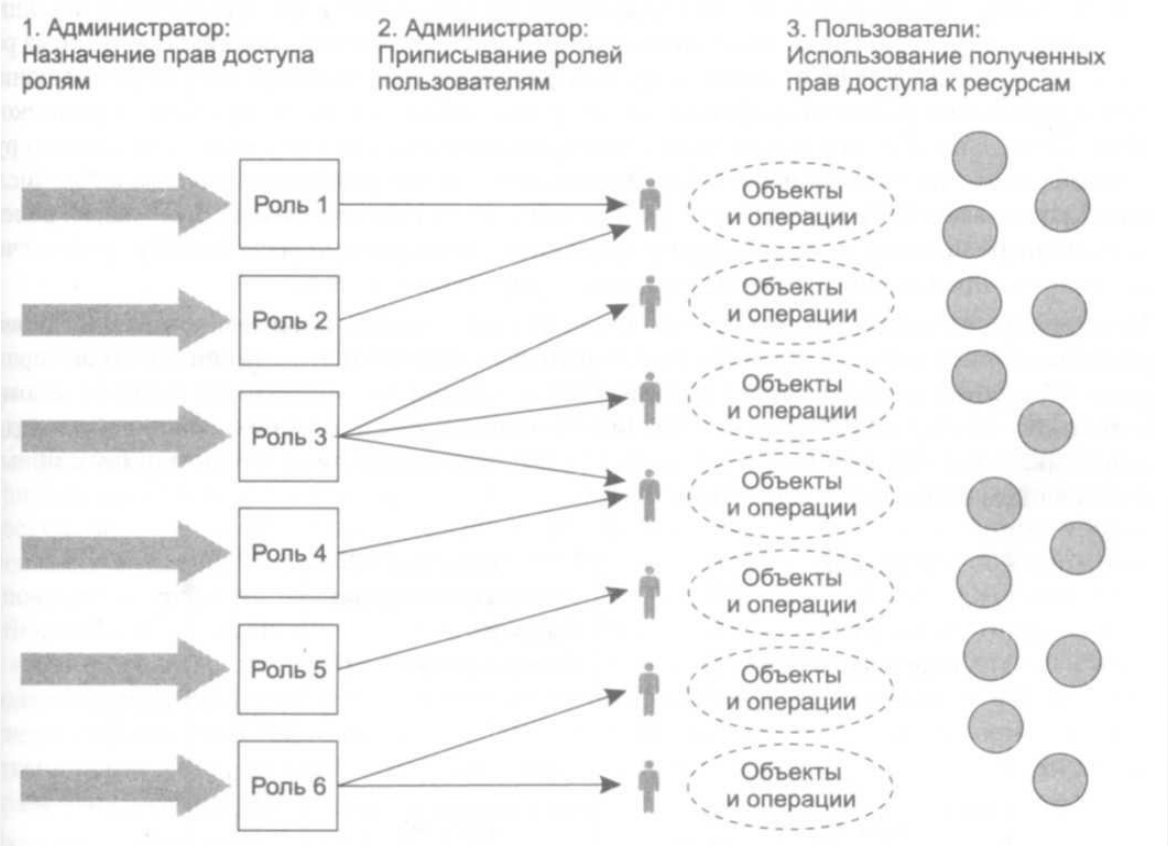
**Ролевое управление доступом** использует роли, которые по сути соответствуют понятиям «должность» и «круг должностных обязанностей».

Набор ролей должен соответствовать перечню различных должностей , существующих на предприятии.

Одна и та же роль может быть приписана разным субъектам.

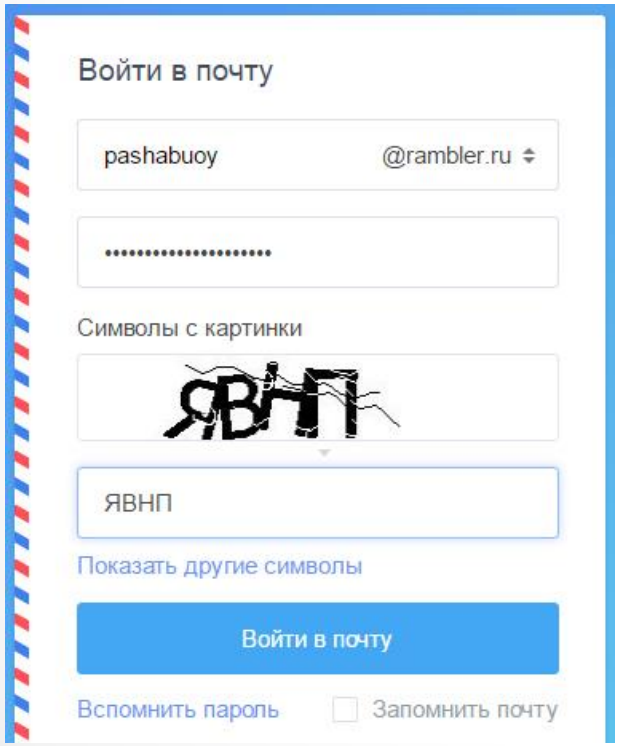
# Принципы организации разграничения доступа

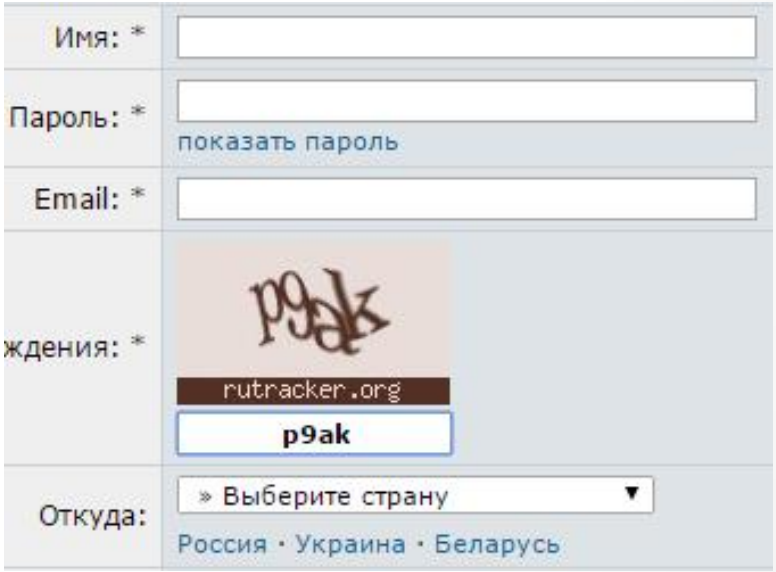
Схема авторизации в системах управления доступом на основе ролей



# Применение методов разграничения доступа

Популярной мерой ограничения доступа в сеть Интернет является **капча** (**Capcher**).



# Применение методов разграничения доступа

Пример дискреционного управления доступом на железнодорожной станции Ипуть БелЖД

| Действия субъектов согласно ПРД | Субъекты информационной системы | | | | | |
|---|---|---|---|---|---|---|
| | начальник станции | дежурный по станции | начальник участка СЦБ | старший электромеханик | электромеханик | диспетчер отделения дороги |
| Получение информации о поездной обстановке на станции | + | + | + | + | + | + |
| Получение специальной технологической информации по станции | + | + | – | – | – | – |
| Получение диагностической информации о системе ПРЦ по фиксированным запросам | – | – | + | + | + | – |
| Управление объектами станции с обеспечением условий безопасности движения поездов | + | + | – | – | – | – |
| Техническое обслуживание объектов управления на станции | – | – | + | + | + | – |
| Обслуживание технических средств ПРЦ | – | – | + | + | + | – |

# 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**