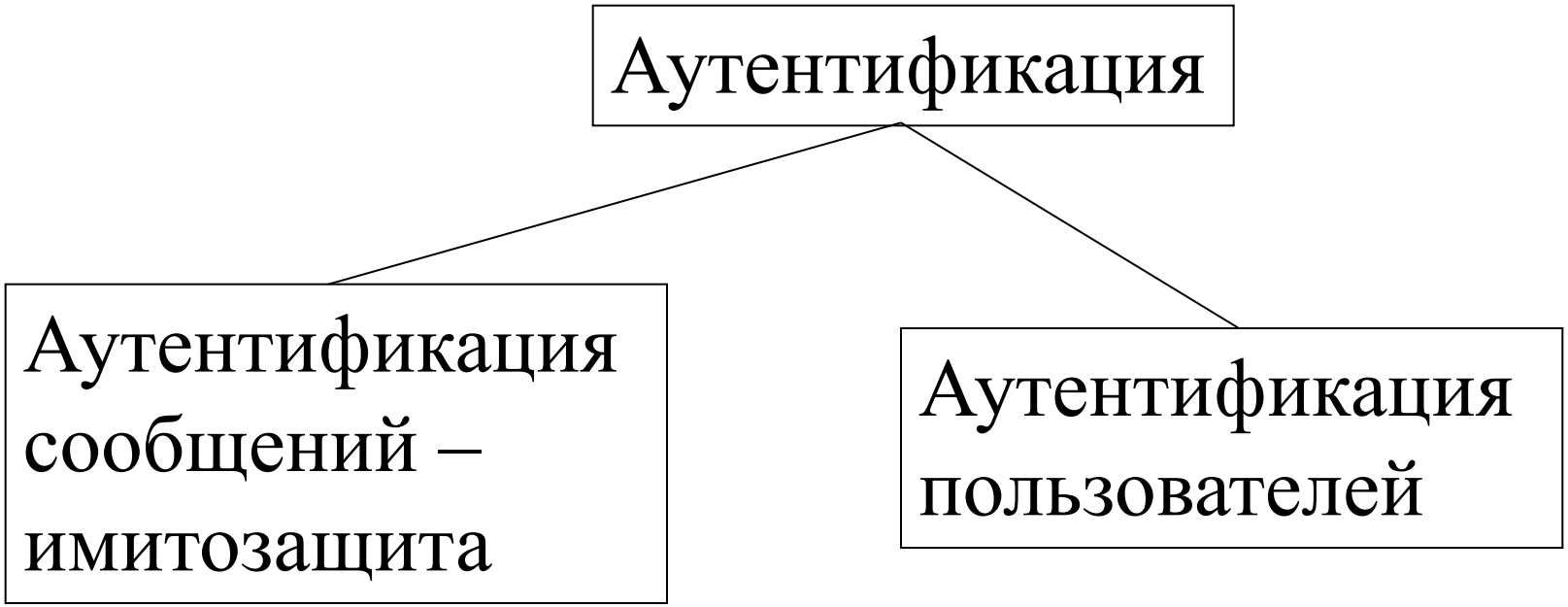
Лекция
Аутентификация сообщений и пользователей компьютерных систем

Лектор: профессор Яковлев В.А.

Виды аутентификации

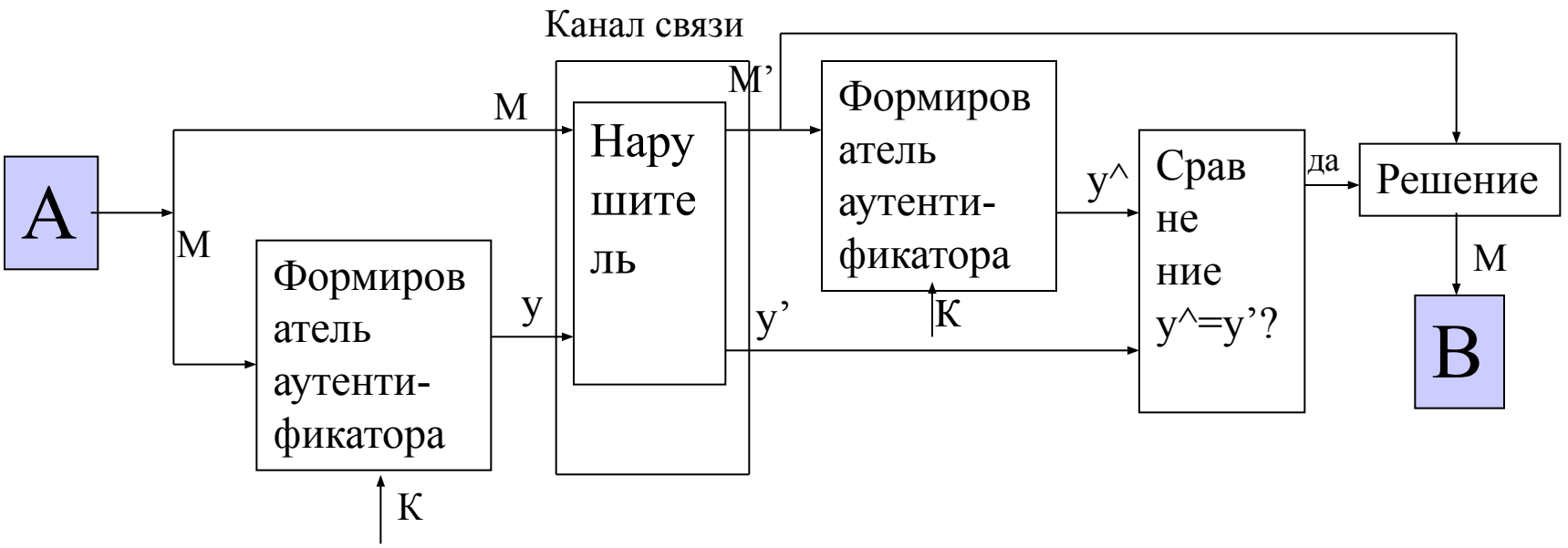


Аутентификация сообщений

Аутентификация сообщений (имитозащита) - обеспечение подлинности передаваемых сообщений

Аутентификация самостоятельное криптографическое преобразование, которое может применяться независимо от других криптографических преобразований, например, шифрования.

Модель передачи сообщений с имитозащитой



Аутентификатор (имитовставка, группа имитозащиты)
y=f(M,K)

Оценки стойкости имитозащиты

Для осуществления навязывания ложного сообщения нарушитель может использовать две стратегии:

1. **Стратегия имитации** - формирование ложной кодограммы (сообщение + имитовставка), не ожидая перехвата настоящей кодограммы.

Вероятность успешной имитации -$P_{и.}$

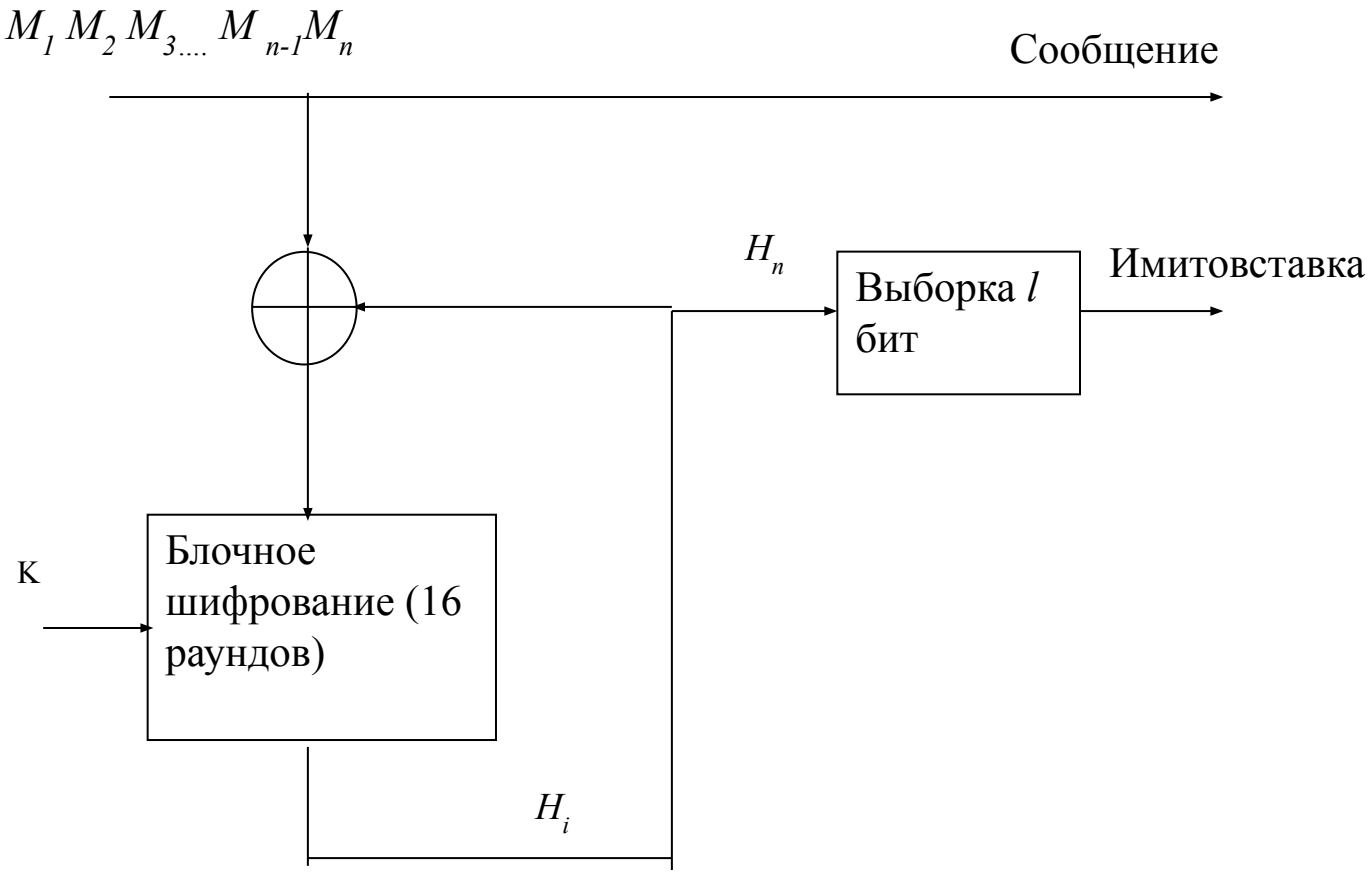
2. **Стратегию подмены** -формирование ложной кодограммы после перехвата подлинной кодограммы.

Вероятность успешной подмены – $P_{п}$

Вероятность навязывания $P_{н}=\max(P_{и}, P_{п})$

Для правильно построенной системы имитозащиты $P_{н}<2^{-l}$, где l – длина имитовставки.

Выработка имитовставки согласно ГОСТ 28147-89



Аутентификация пользователей (корреспондентов)

Аутентификация –метод, позволяющий достоверно убедиться в том, что субьект действительно является тем за кого себя выдает.

Идентификация – присвоение уникального имени (идентификатора) позволяющему субъекту назвать себя на соответствующий запрос системы.

Субъект может подтвердить свою подлинность , если предъявит одну из следующих сущностей:

-нечто, что он знает (пароль, личный идентификатор, криптоключ).

-нечто, чем он владеет (пластиковая карта);

-нечто, что является частью его самого (голос, отпечаток пальца и т.п.

Способы аутентификации, основанные на знании субъектом уникальной информации

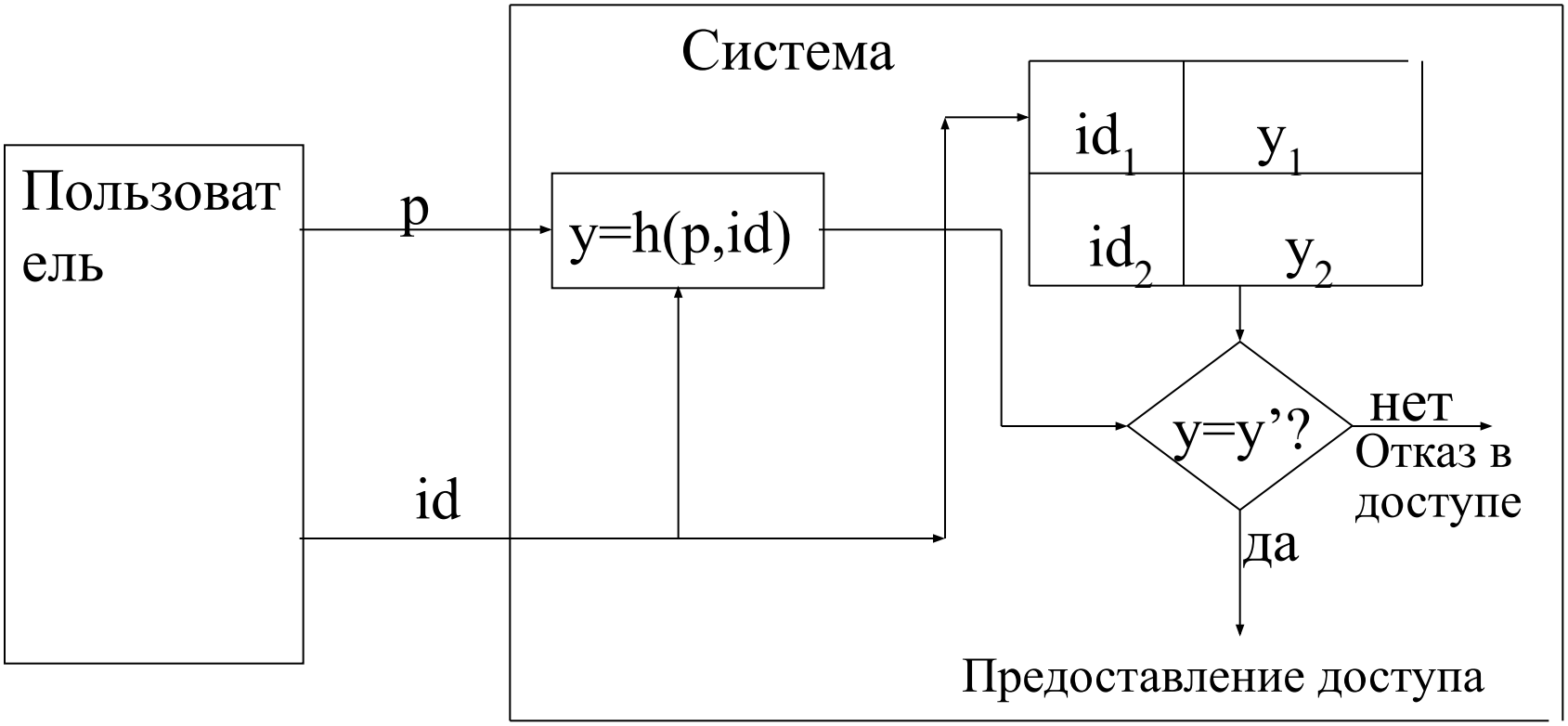
Способ паролирования;
Способ запрос-ответ;
Способ рукопожатия;
Способ, использующий сервер аутентификации;
Способ, основанный на сертификатах открытых ключей.

Паролирование

Угрозы безопасности для паролирования

1. Компрометация пароля при его неправильном хранении.
2. Угадывание пароля, если он короткий и неслучайный.
3. Пассивный перехват при вводе и передаче по линиям связи.

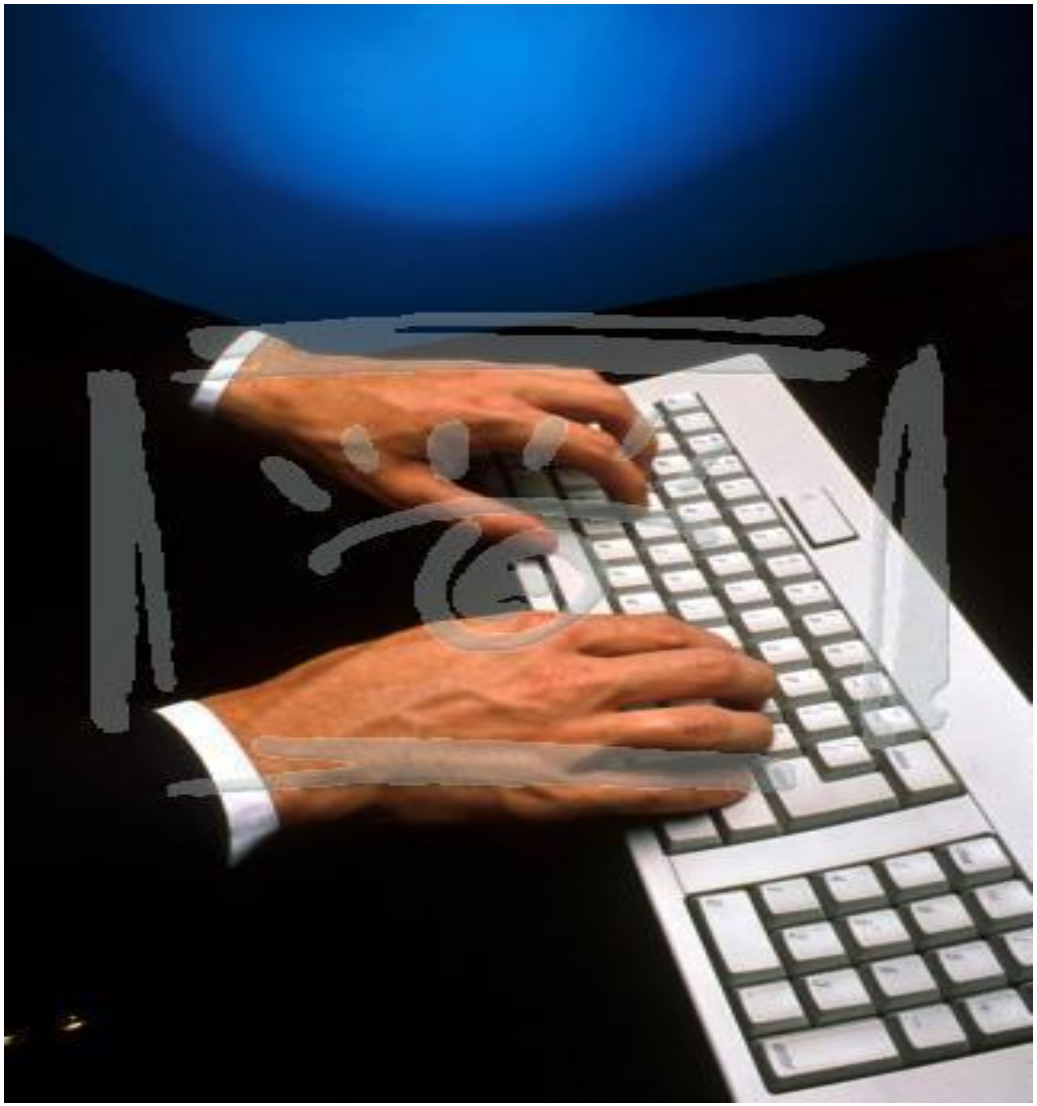
Хэширование паролей при хранении



Проблема паролирования

- Человек может запомнить относительно короткий пароль - 6-8 символов. Множество паролей фиксировано.
- Быстродействие вычислительной техники постоянно увеличивается и поэтому время для подбора правильного пароля уменьшается.

Пример для графического пароля, предложенного G.E.Blonder.



Подсматривание пароля

Генерируемая сцена аутентификации


Form
R
Refresh

Пусть $Z = \frac{1}{N}\sum_{j=1}^{N} y_{ji}$ – среднее выборочное для i-го типа знака за N – наблюдений. i={0,1}, где 0 – соответствует выбору не парольного знака, 1- выбору парольного знака.

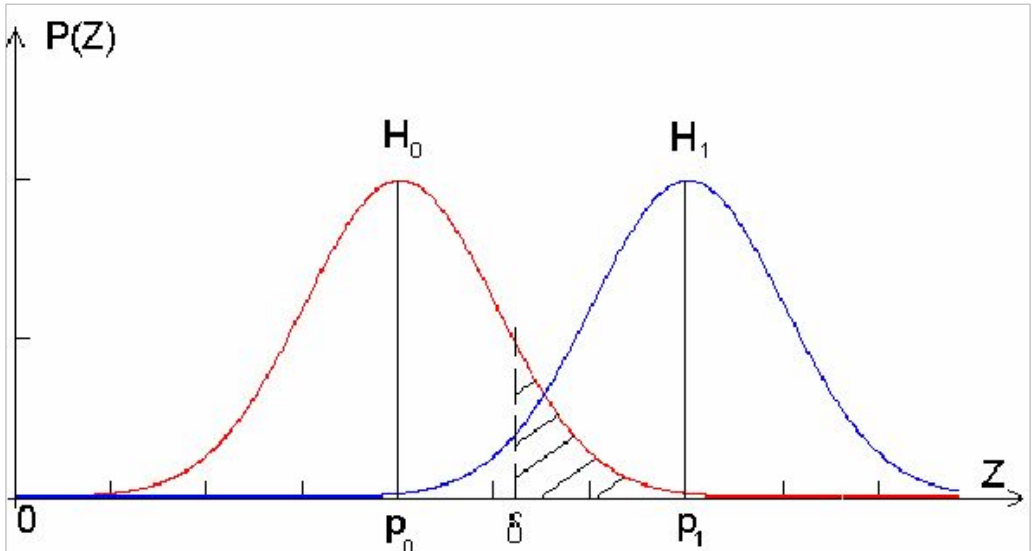
При достаточно большом N случайная величина Z будет иметь гауссовское распределение с параметрами:

M{Z}=p_i, и $D\{Z\} = \frac{\sigma_i^2}{N}$, где σ_i^2 - дисперсия выбора i-го знака.

Задача определения типа знака сводится к задаче различения двух гипотез:

H_0 – наблюдаемы знак не парольный,

H_1 – наблюдаемый знак парольный.



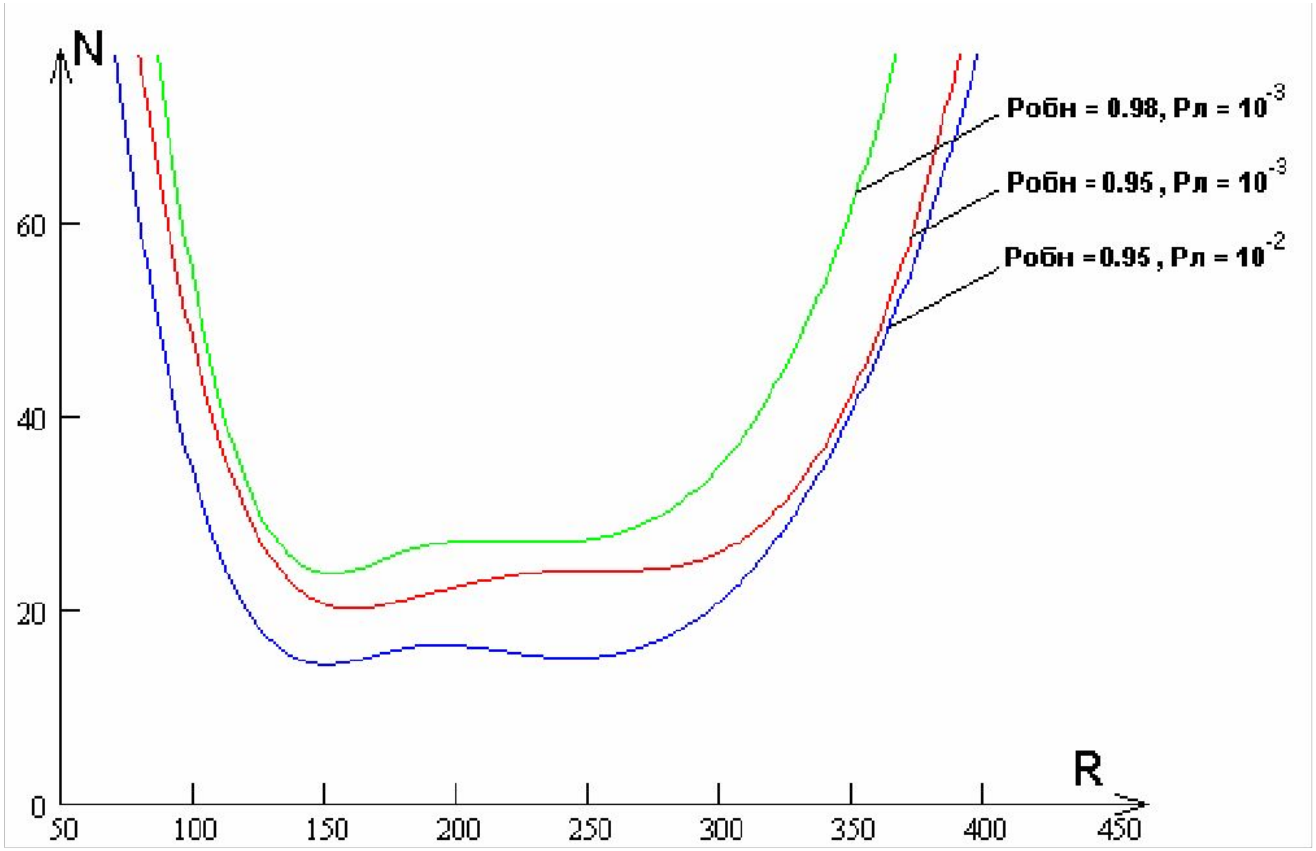
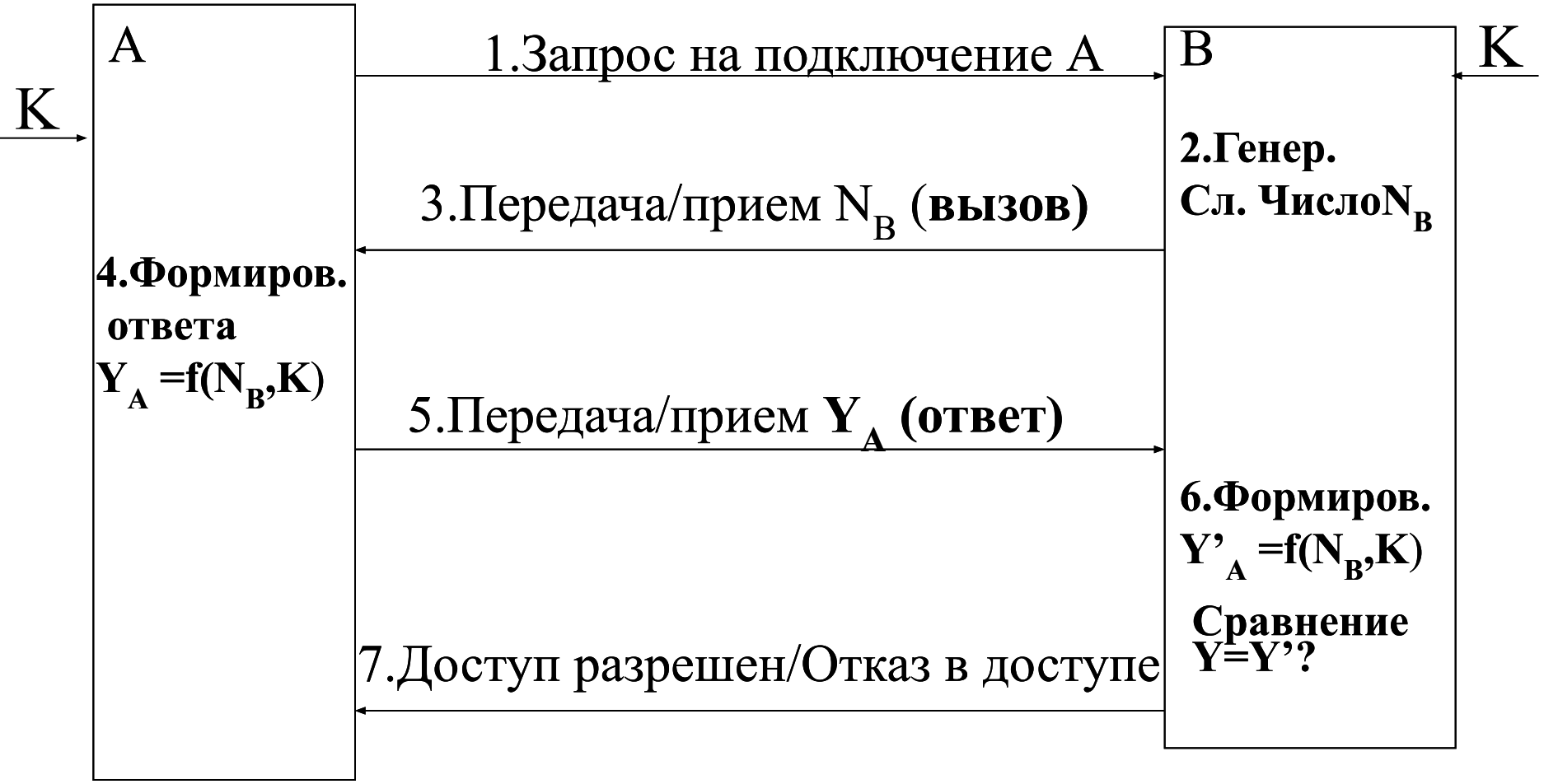


Рис. 3.15. Зависимость числа подсматриваний от радиуса.

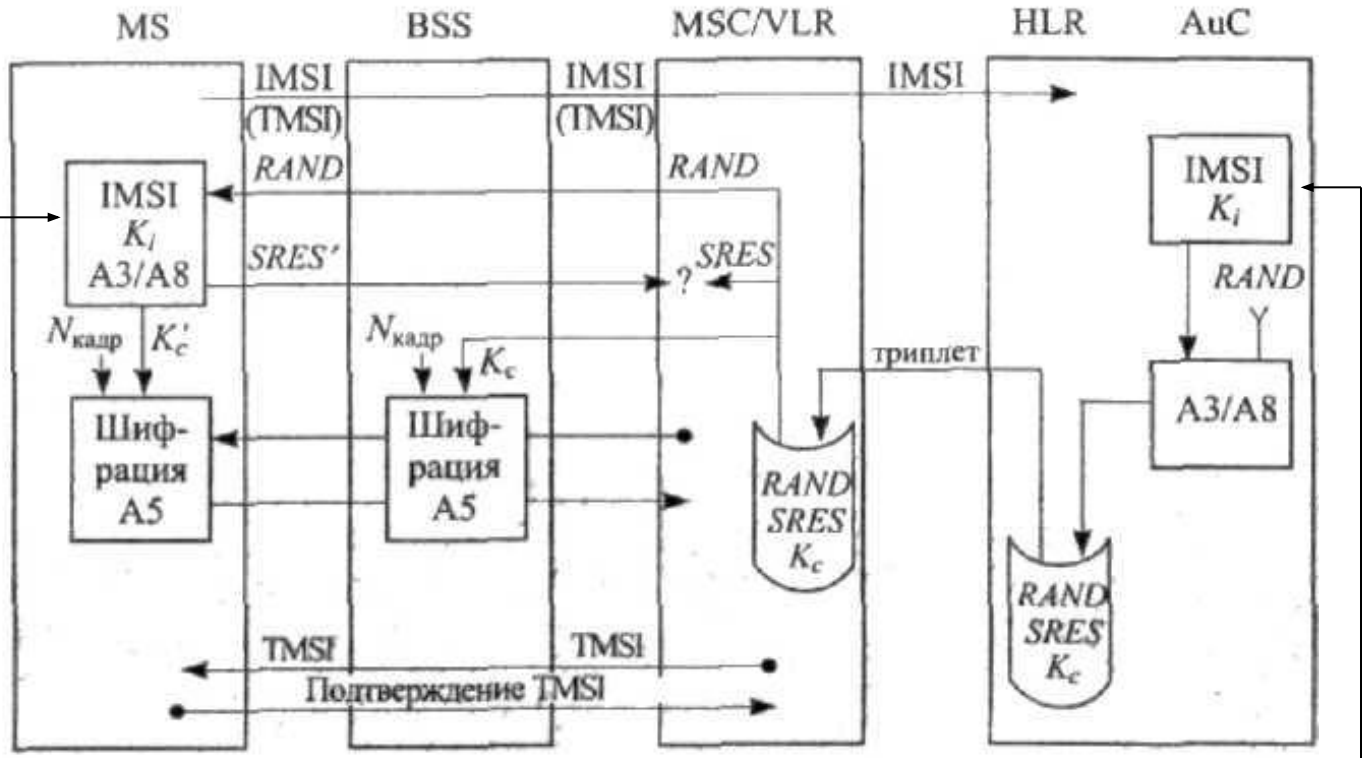
Одноразовое паролирование, протокол S/Key

K – парольная фраза

Аутентификация способом вызов-ответ



Безопасность информации в G2 системе

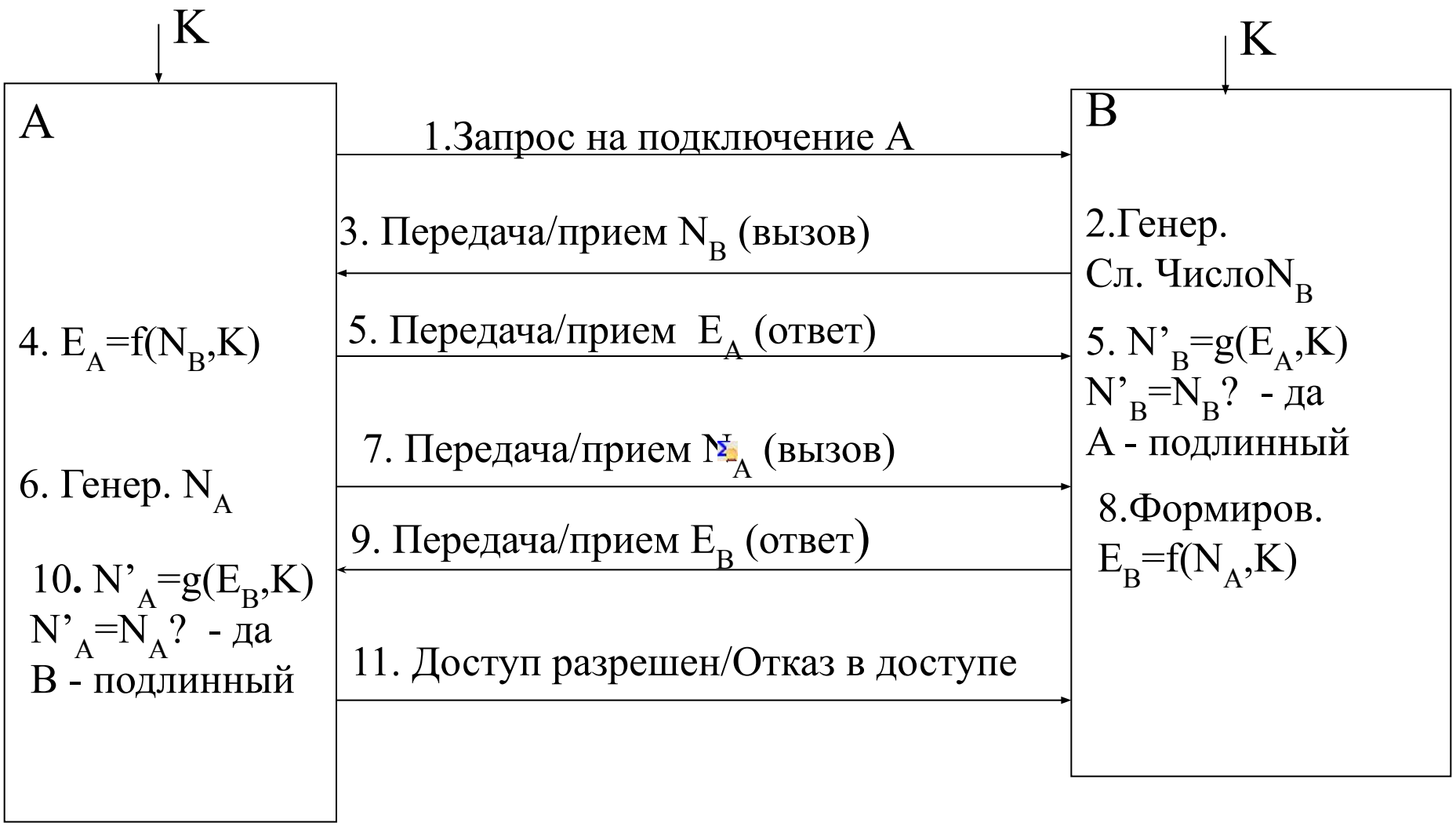


Абонент

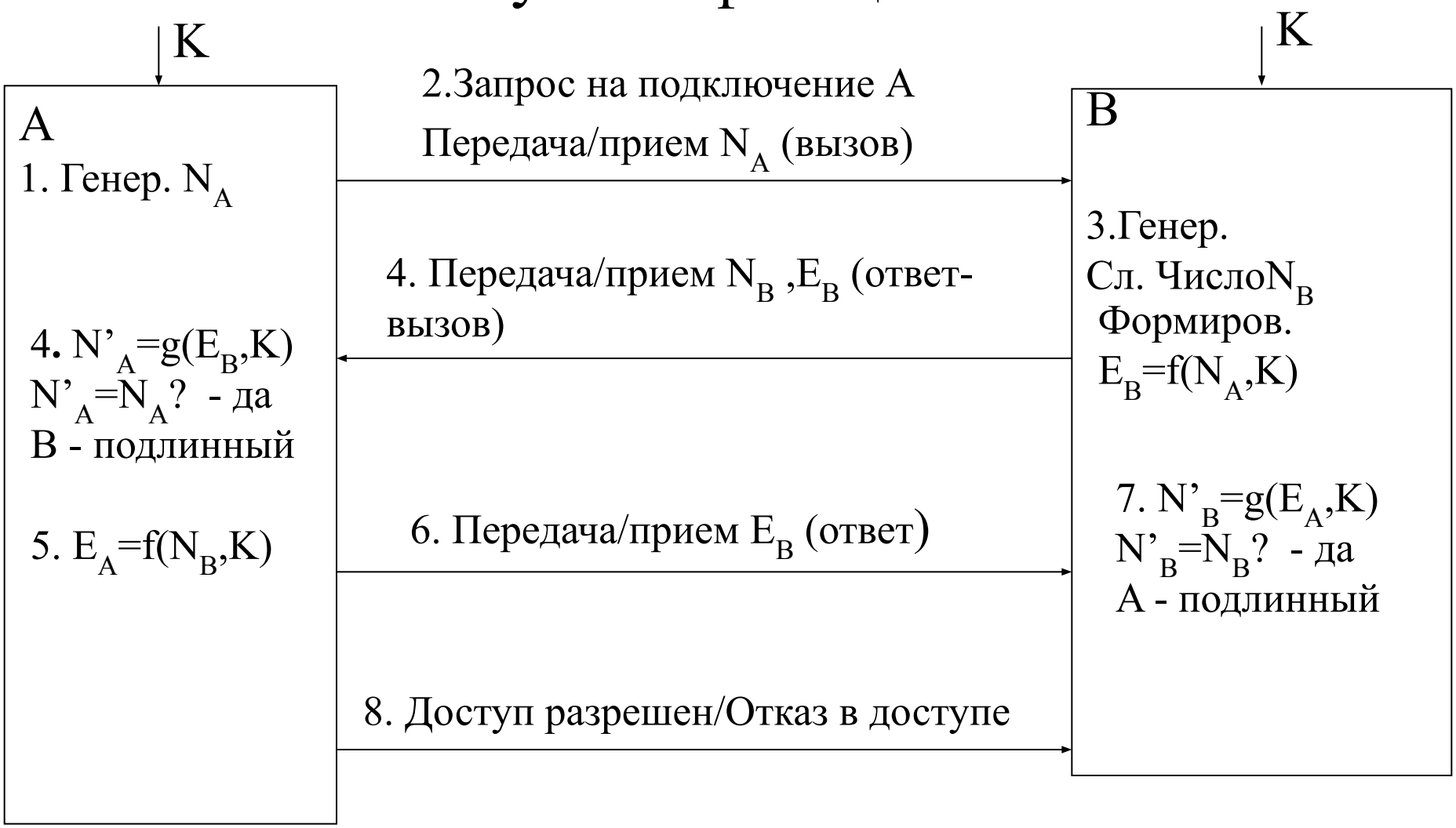
Пункт регистрации

Центр формирования ключей и идентификационных номеров (WSISDN,..) (Ki, IMSI), PIN, SIM(Ki, IMSI),

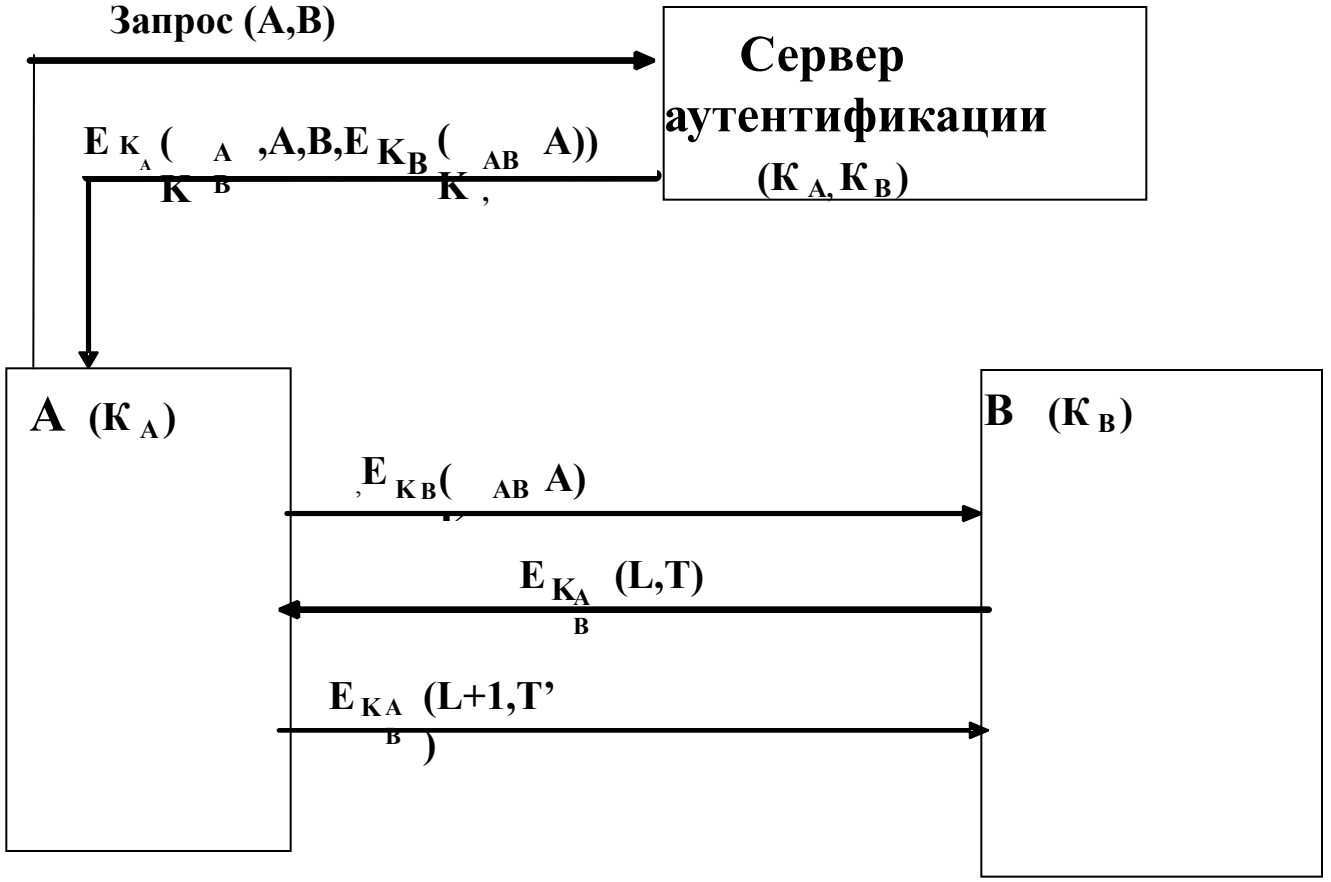
Аутентификация способом рукопожатия



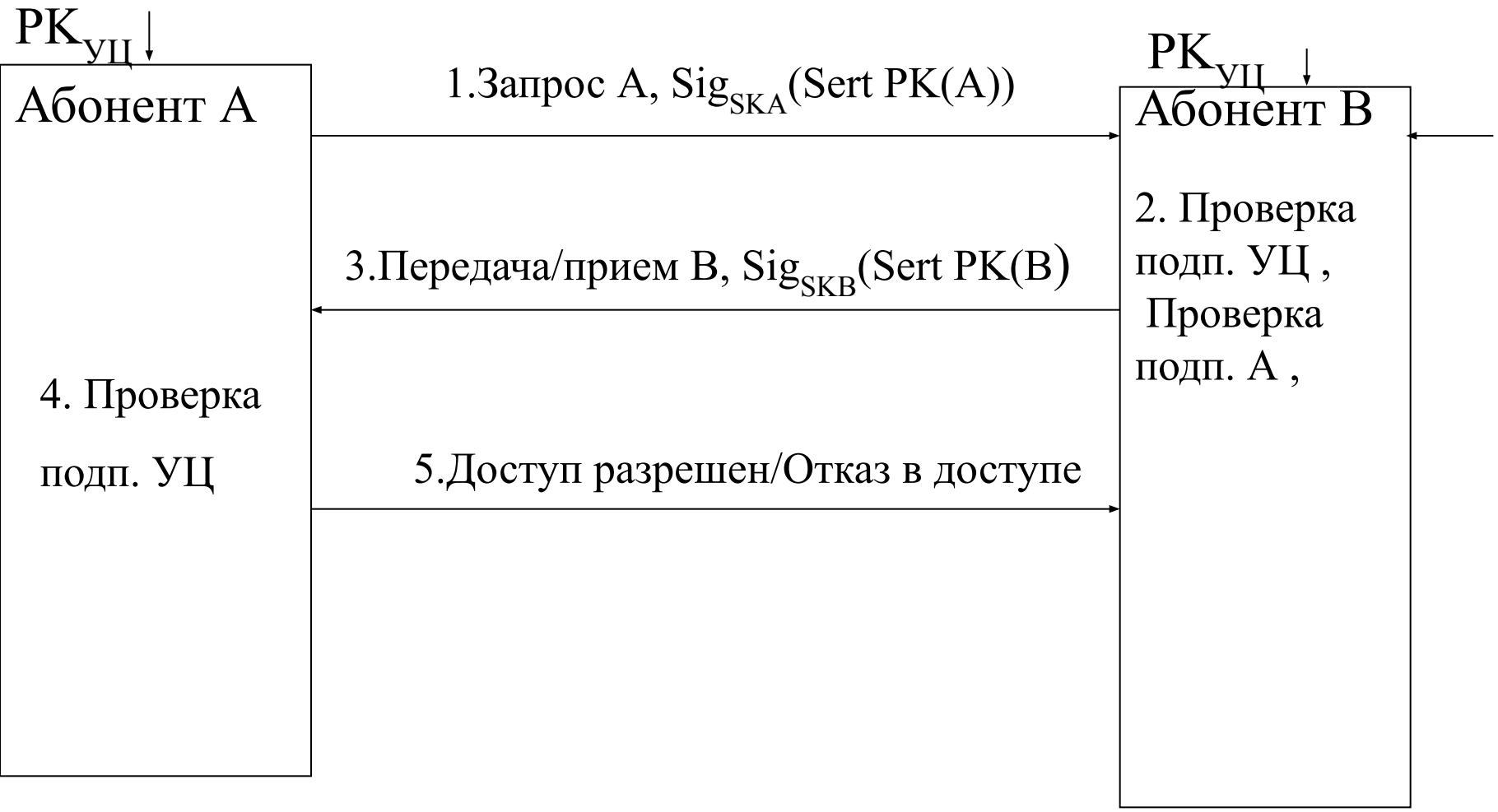
Укороченная двухсторонняя аутентификация



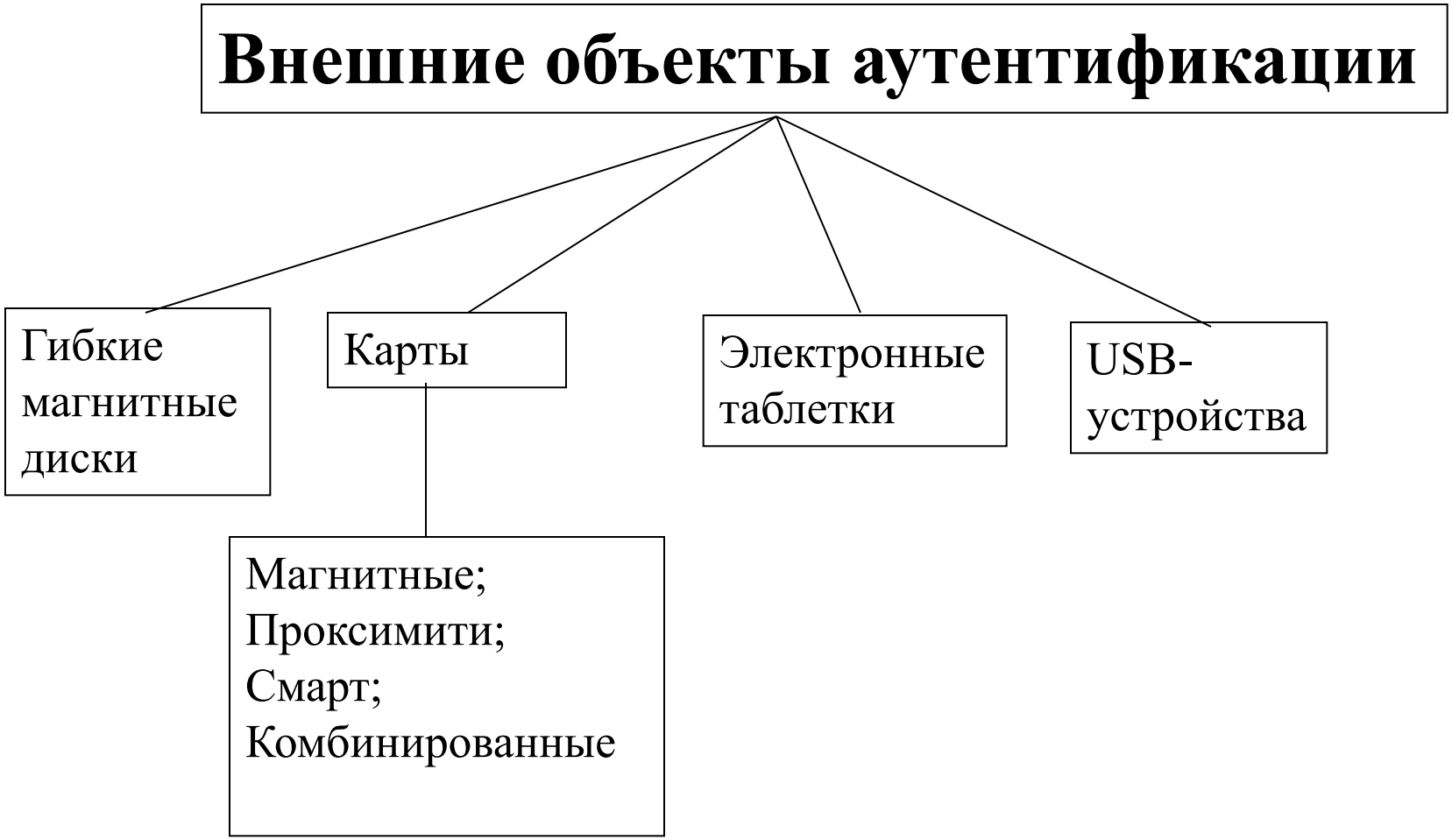
Аутентификация и распределение ключей с использованием сервера аутентификации



Аутентификация с использованием сертификатов открытых ключей



Внешние объекты аутентификации



Магнитная карта

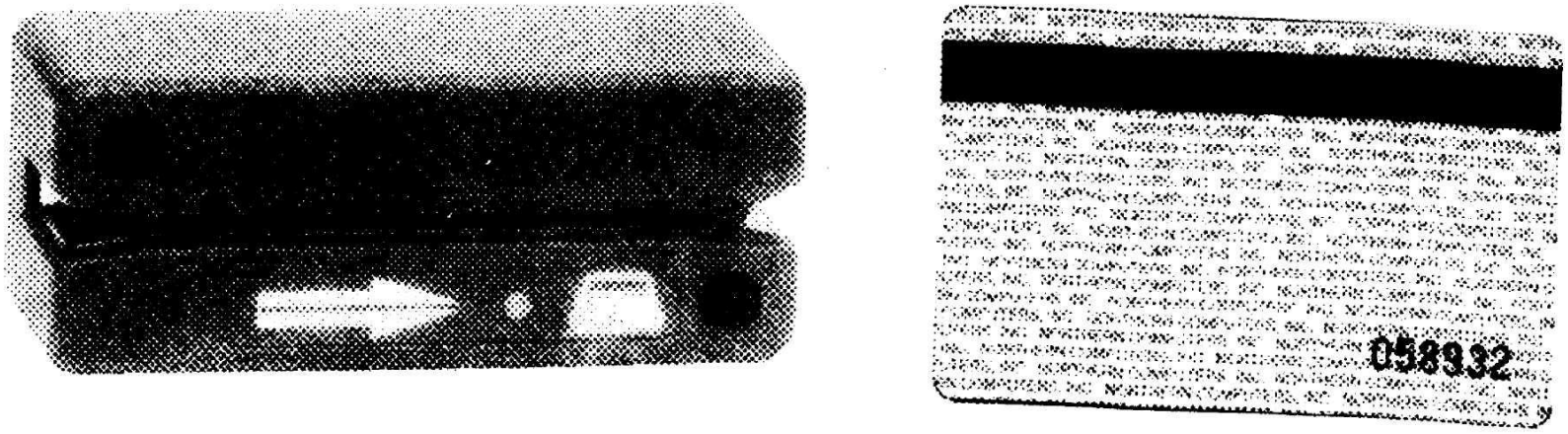


Рис. 3.55. Считыватель карт с магнитной полосой и карта

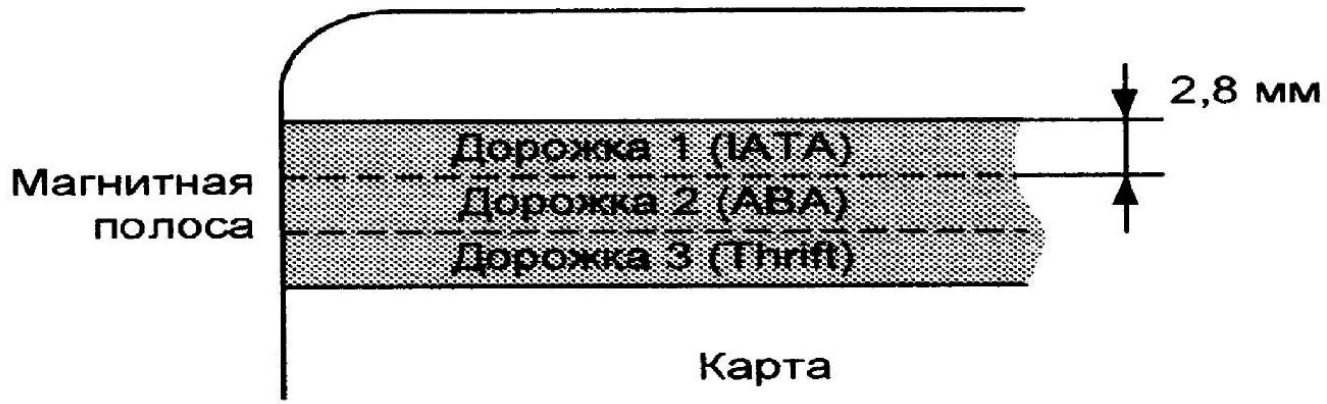


Рис. 3.52. Размещение дорожек на магнитной полосе карты

Проксимити карта

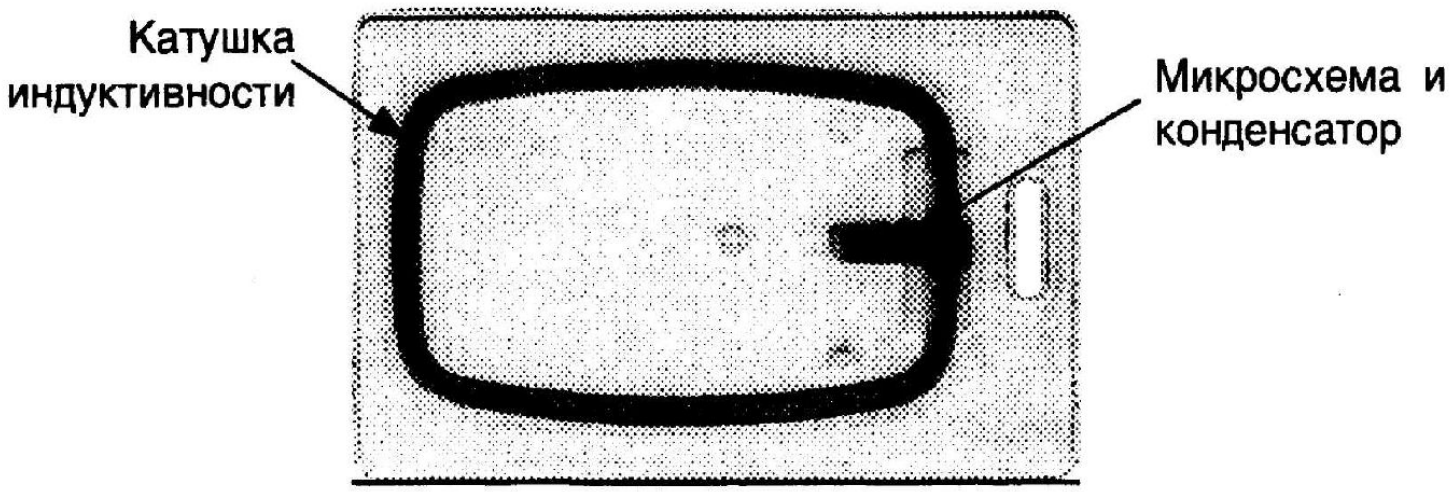


Рис. 3.21. Устройство карты радиочастотной идентификации (проксимити)

Функциональная схема считывателя и карты

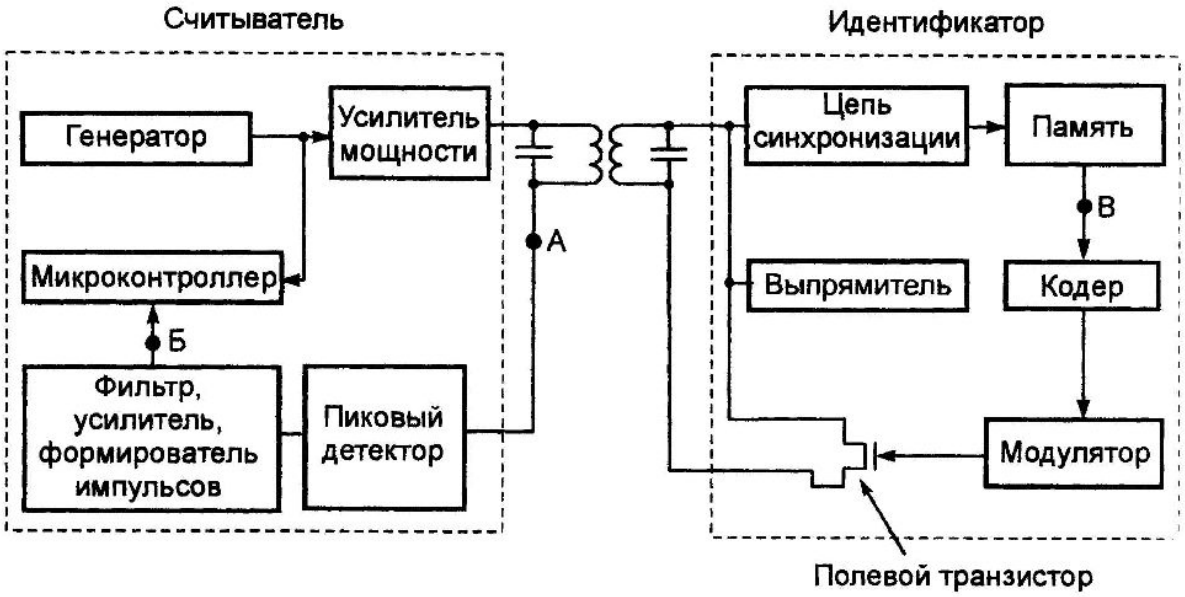


Рис. 3.25. Функциональная схема радиочастотного устройства идентификации

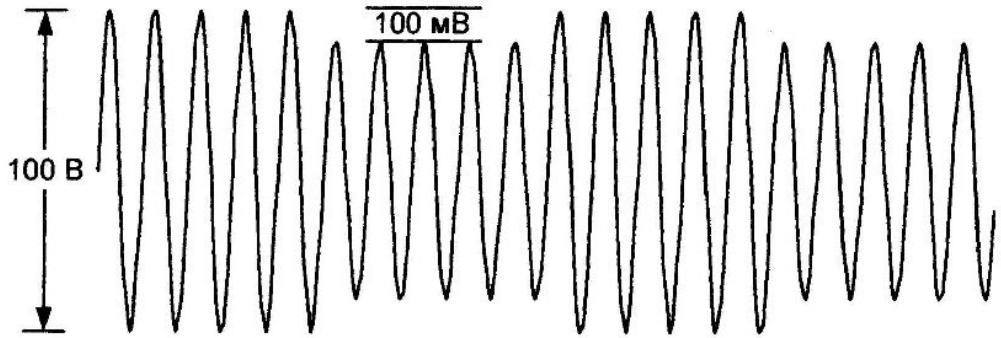


Рис. 3.26. Амплитудно-модулированный сигнал

Смарт-карта

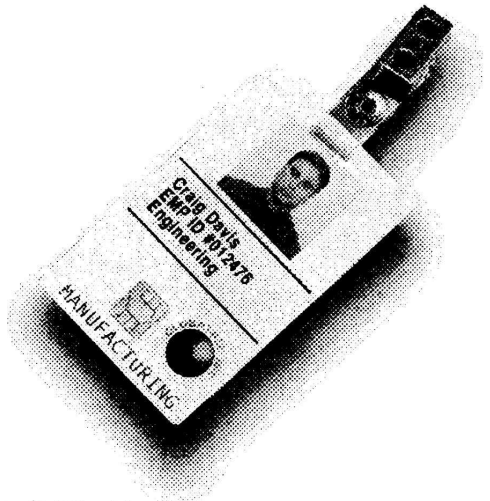


Рис. 3.59. Контактная смарт-карта

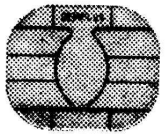
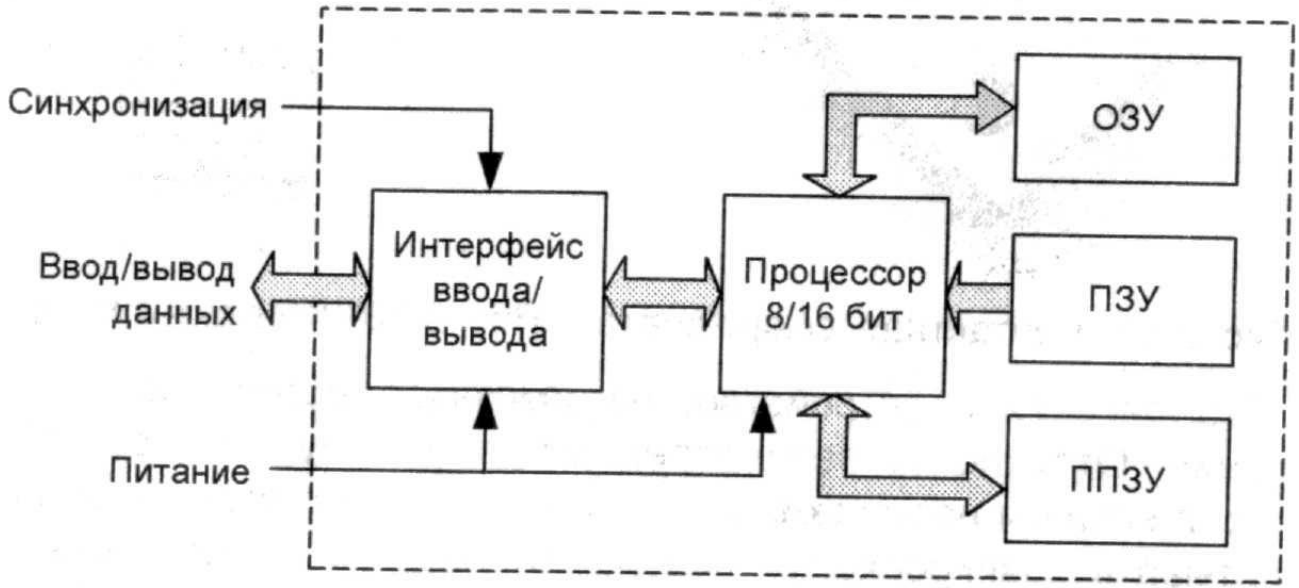


Рис. 3.60. Контакты микросхемы



Бесконтактная смарт-карта

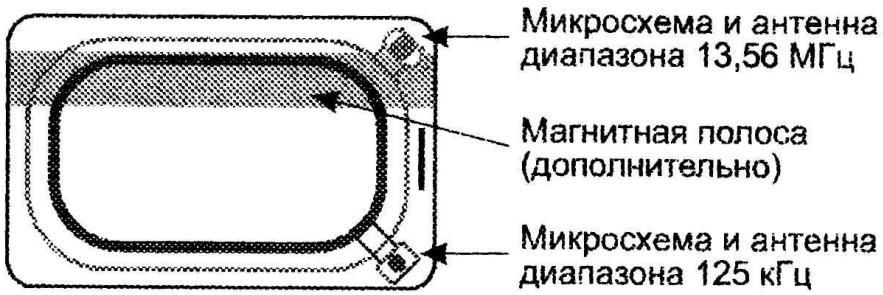


Рис. 3.56 Комбинированная бесконтактная смарт-карта

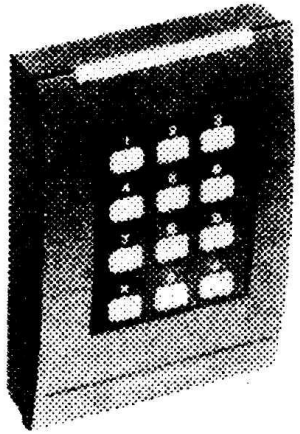


Рис. 3.57. Пример считывателя бесконтактных смарт-карт, совмещенного с клавиатурой

Электронная таблетка

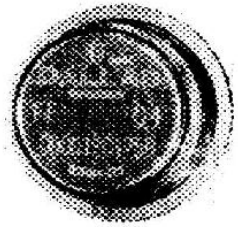


Рис. 3.57. Электронная таблетка

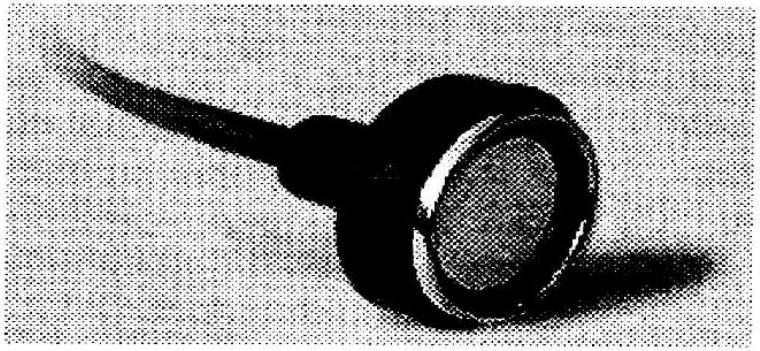
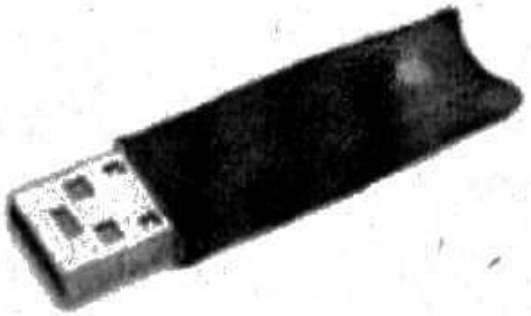


Рис. 3.58. Считыватель

Электронные ключи



Характеристики USB-ключей

Изделие	*Емкость памяти, Кб*	*Разрядность серийного номера*	*Встроенные алгоритмы шифрования*
eToken R2	16/32/64	32	DESX (ключ 120 бит), MD5
eToken Pro	16/32	32	RSA/1024, DES, 3DES (TripleDES), SHA-1
iKey l0xx	8/32	64	DES (режимы ECB и CBC), DESX, 3DES, RC2, RC4, RC5, MD5
iKey 20xx	8/32	64	DES (режимы ECB и CBC), DESX, 3DES, RC2, RC4, RC5, RSA/1024
ePass 1000	8/32	64	MD5, MD5-HMAC
ePass 2000	16/32	64	RSA, DES, 3DES, DSA, MD5, SHA-1
WebIdentity	16/32	32	3DES, MD5
CryptoIdentity	32	32	RSA/1024

Технические характеристики eToken RIC

Спецификация на eToken RIC

Название модели	eToken RIC
1	*2*
ATR	3b 65 00 00 ac e1 01 23 00
Тип контроллера	8-ми разрядный, с RISC-архитектурой
Производительность микроконт-роллера	До 5 КБ в секунду (ГОСТ 28147-89)
Компонент перезапуска (Reset)	Интегрирован в процессор
Поддержка спящего (Suspend) ре-жима USB	Да
Алгоритмы шифрования	DES, 3DES, ГОСТ 28 147-89
Диверсификация, имитозащита, формирование сессионного ключа	ГОСТ 28147-89

Биометрические признаки

Квазистатические

- Отпечаток пальца;
- Форма кисти руки;
- Геометрия лица;
- Рисунок сетчатки глаза;
- Рисунок радужной оболочки глаза;
- Код ДНК

Квазидинамические

- Параметры речи;
- Параметры пульса;
- Подпись и динамика ее воспроизведения;
- Параметры походки;
- Динамика (стиль) работы на рабочей станции

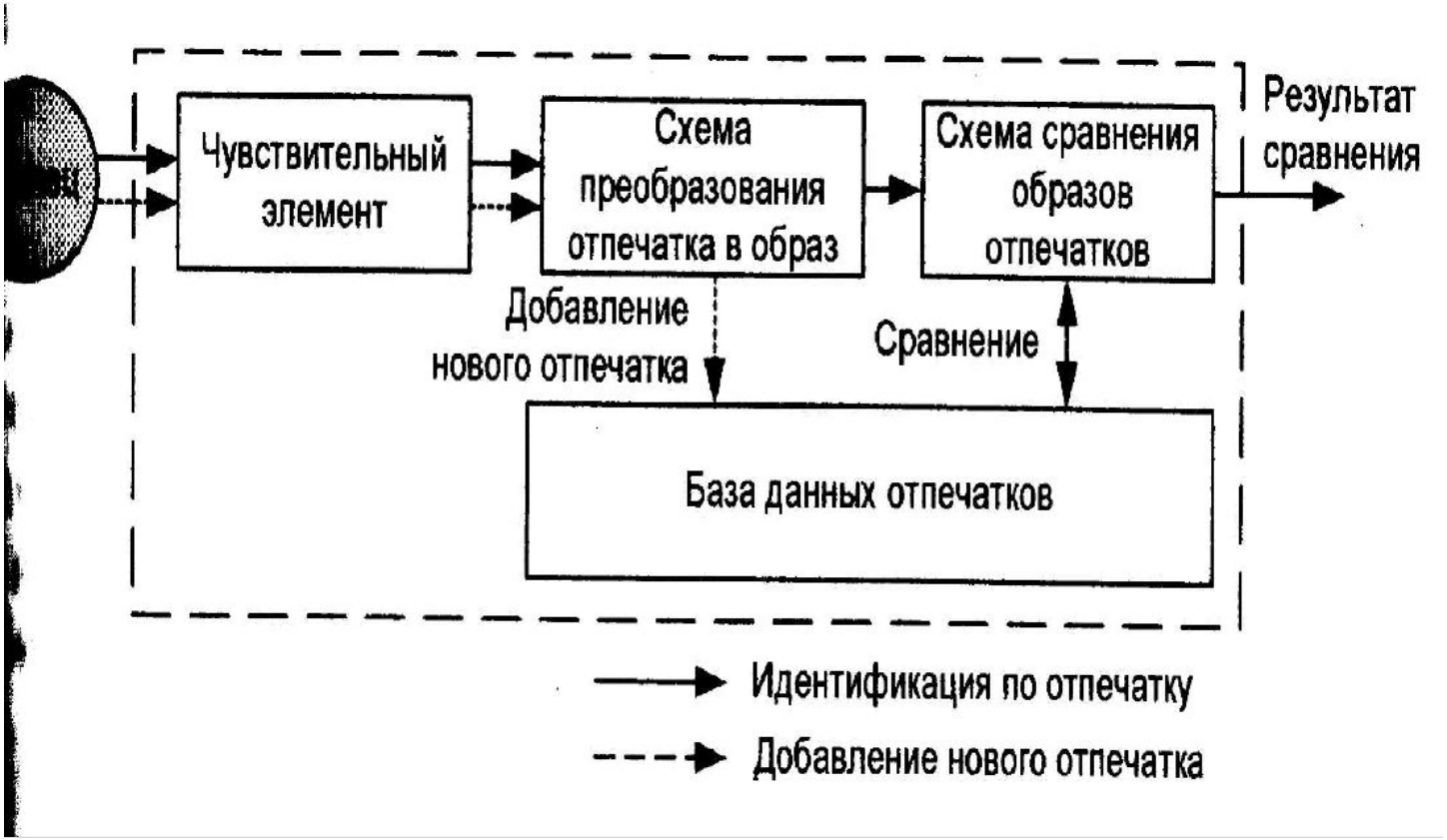
Характерные особенности отпечатка пальцев

Рис. 3.4. Характерные особенности отпечатка пальца

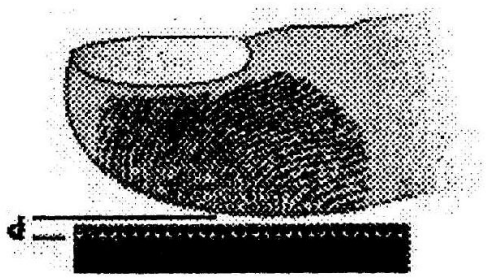
Рис. 3.5. Набор характерных точек

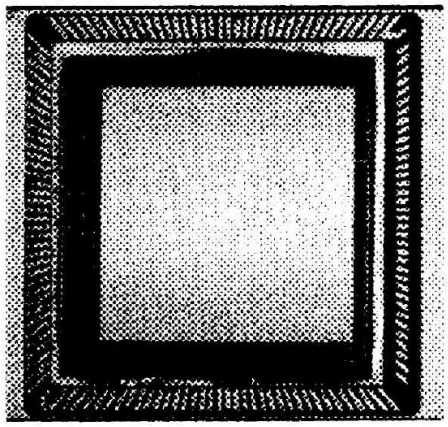
путем сравнения

Структурная схема считывателя отпечатков пальца



Полупроводниковый считыватель





Считыватели отпечатков пальцев

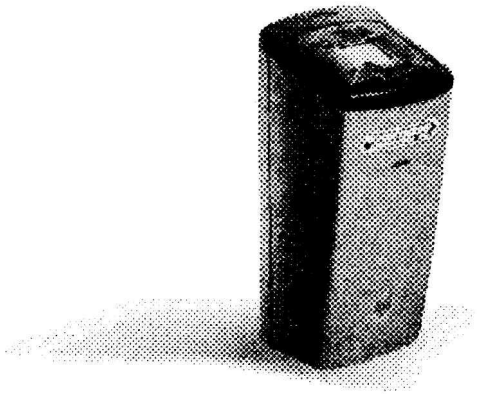


Рис. 3.8. Считыватель отпечатков пальцев VeriPass

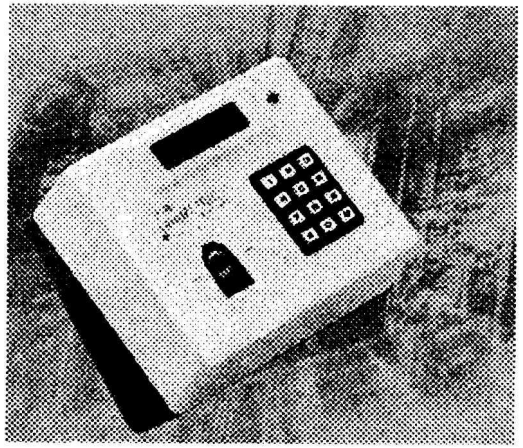


Рис. 3.9. Считыватель отпечатков пальцев, совмещенный с клавиатурой

БИОМЕТРИЧЕСКИЙ СКАНЕР

Сканер MAGICSECURE 2000 обеспечивает аутентификацию пользователя по его отпечатку пальца.

Обеспечивает доступ зарегистрированных пользователей к информации и услугам компьютерной сети.

Подключение через USB-порт.

ОПТИЧЕСКАЯ МЫШЬ С ИДЕНТИФИКАЦИЕЙ ПО ОТПЕЧАТКУ ПАЛЬЦА

Мышь MAGICSECURE 3100 обеспечивает быстрое распознавание законного пользователя рабочей станции.

ОСОБЕННОСТИ:

* **Двухфактурная аутентификация (отпечаток пальца, пароль);**
* **Гибкая регистрация;**
* **Подключение через USB-порт;**

ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ:

	Сканер	Оптическая мышь
* Время проверки:	менее 0,3 с	менее 1 с
* Время регистрации:	менее 0,9 с	менее 3 с
* Вероятность неподтверждения:	0,1%	0,01%
* Вероятность неправильного подтверждения:	0,01%	0,001%
* Размер шаблона:	256 байт	
* Разрешающая способность:	508 dpi	

Биокриптофлэш

Назначение: - персональное средство криптографической защиты информации с биометрической технологией доступа по отпечатку пальца.

Алгоритм шифрования - **ГОСТ 28147-89.**

Процесс шифрования и аутентификации пользователя полностью реализован внутри устройства без применения ресурсов ПЭВМ.

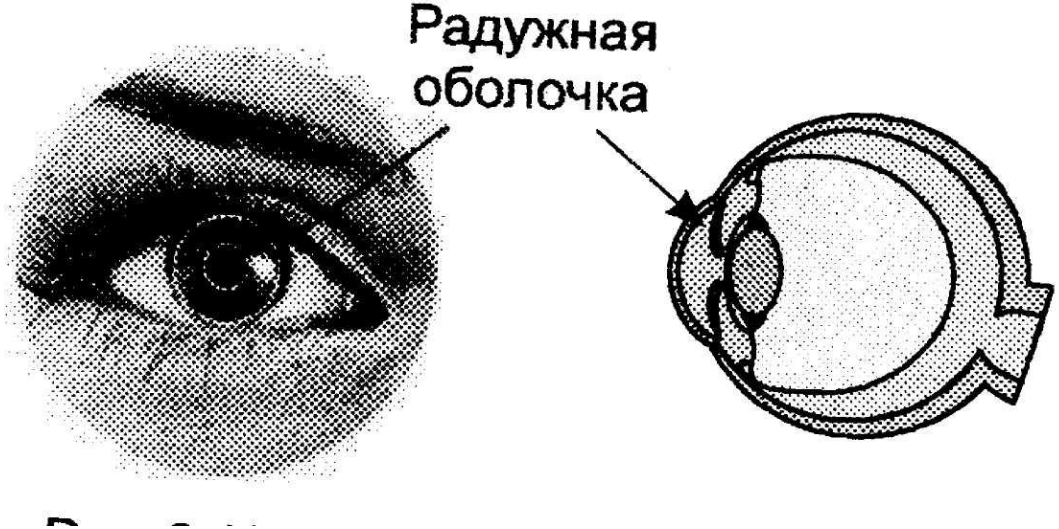
Аутентификация пользователя: по отпечаткам пальцев с применением пароля пользователя или без него.

Поддерживает работу с ОС Windows.

Характеристики считывателей

Модель	V-Pass	V-Prox	V-Smart	BioAccess
Фирма-производитель	*Bioscrypt*	*Bioscrypt*	*Bioscrypt*	*Northern Computers*
Технология считывания	Только отпечаток	Карта + отпечаток (хранится в считывателе)	Карта + отпечаток (хранится на карте Mifare)	Карта + отпечаток (хранится на карте Mifare)
Поддерживаемые интерфейсы	Виганда, RS-232, RS-485			Виганда, магнитных карт, RS-232, RS-485
Типы карт для считывателя	–	26 или 34 бит HID	Mifare Standard	Mifare Standard
Количество пользователей в системе	100 (возможность расширения до 200)	4500	Не ограничено	Не ограничено
Время добавления нового пользователя	Менее 3 с	Менее 3 с	Менее 5 с	Менее 10 с
Время идентификации пользователя	Менее 1 с (при 100 отпечатках)	Менее 1 с	Менее 2 с	Менее 1 с
Вероятность несанкционированного доступа ($P_{н.д}$)	0,002	–	–	Менее 0,0005
Вероятность ложного отказа в доступе ($P_{л.о}$)	0,01	–	–	Менее 0,01
Эквивалентная вероятность ошибки (EER)	–	0,001	0,001	–
Напряжение питания	7–24 В пост. тока		8–12 В пост.тока	12–24 В пост.тока
Потребляемый ток в дежурном режиме	200 мА при 12 В	60 мА при 12 В	200 мА при 12 В	110 мА при 12 В
Потребляемый ток в режиме добавления пользователей	250 мА при 12 В	250 мА при 12 В	250 мА при 12 В	250 мА при 12 В
Размеры, мм	130x50x65,5		130x118x63,5	125x68x61

Радужная оболочка глаза



Считыватели радужной оболочки глаза

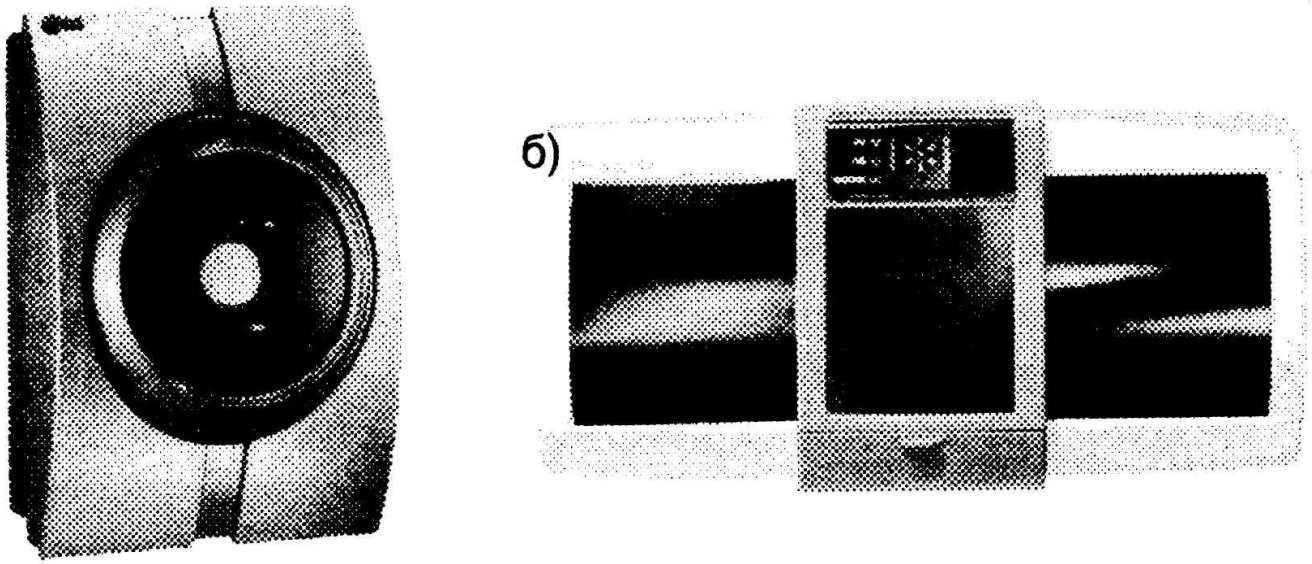


Рис. 3.19. Считыватели радужной оболочки глаза

Сетчатка глаза

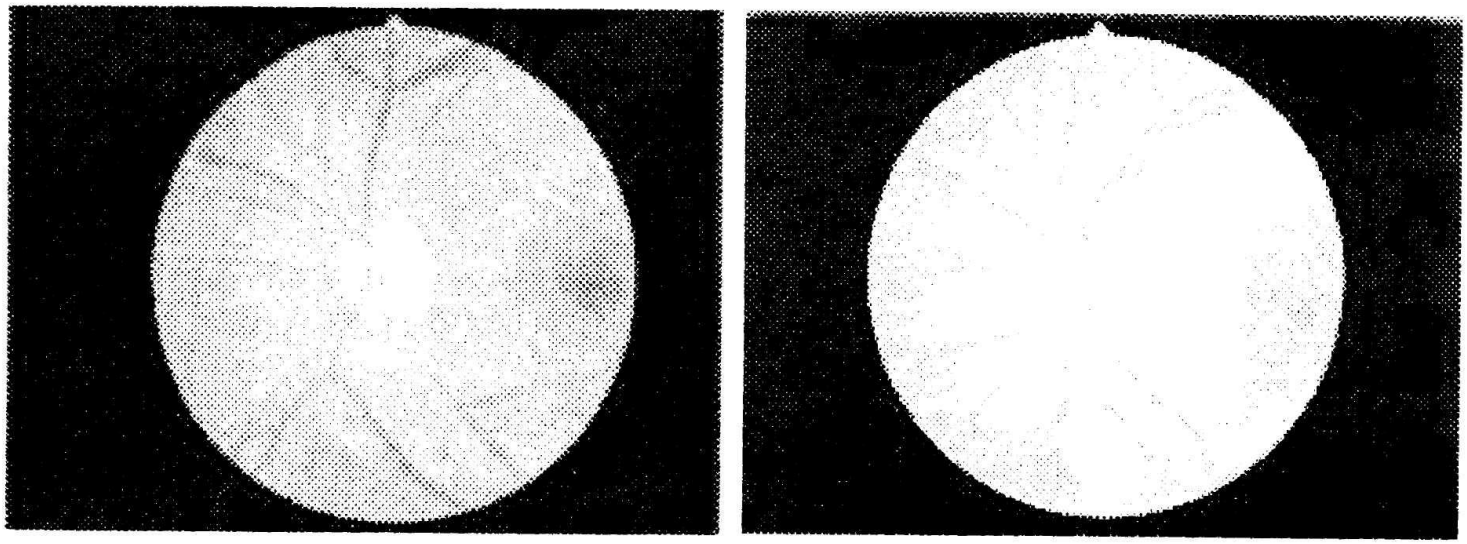


Рис. 3.20. Сетчатки левого глаза у близнецов