Лекция 3. Биометрическая аутентификация

1. Принципы биометрической аутентификации.
2. Создание и проверка биометрических эталонов.
3. Оценка качества биометрической аутентификации.
4. Использование криптографии в системах биометрической аутентификации.

Компоненты систем биометрической аутентификации

- Устройства считывания биометрических характеристик.
- Алгоритмы сравнения измеренных биометрических характеристик с эталонными из учетной записи пользователя.

Проблемы биометрической аутентификации

- Риски ошибочного отказа и допуска (из-за неполного совпадения с эталоном).
- Угроза атак воспроизведения (попыток представления копии характеристики):
  - использование внешнего записывающего устройства;
  - копирование двоичного представления характеристики.
- Угроза атак подделки считываемых данных.

Для защиты требуется усложнение и удорожание устройств считывания.

Применение биометрии

1. Аутентификация (в системах локальной аутентификации или в сочетании со случайными базовыми секретами при удаленном доступе).
2. Идентификация (поиск конкретного лица по измеренной характеристике).
3. Определение уникальности (проверка присутствия проверяемого лица в базе данных получателей пособий, избирателей и т.п.).

Биометрические характеристики

- Физические характеристики человека (статические).
- Поведенческие характеристики (динамические).

- Максимальная уникальность, постоянство в течение длительного периода, отсутствие воздействия состояния человека или косметики.
- Не требуется измерение одного и того же параметра для снижения риска воспроизведения.

Возможно нарушение конфиденциальности частной жизни.

Аутентификация по отпечаткам пальцев

Мышь со

Папиллярные узоры уникальны

Ноутбук со

Силиконовый и оптический сканеры отпечатков пальцев

Поддержка PIN-кодов и смарт-карт для многофакторной аутентификации.

Аутентификация по геометрической форме руки

Камера и несколько подсвечивающих диодов

Аутентификация по радужной оболочке глаза

Преимущества сканирования радужной оболочки:

- образец пятен на радужной оболочке находится на поверхности глаза, и его видеоизображение может быть отснято на расстоянии метра;
- сканирование возможно и у людей с ослабленным зрением, но неповрежденной радужной оболочкой;
- катаракта — повреждение хрусталика глаза, который находится позади радужной

Сканер радужной оболочки глаза

Камера должна оказаться на уровне глаз и на расстоянии 48-53 см от пользователя.
Интерфейс: USB 2.0.

Считыватель радужной оболочки глаза

Конструкция с двойным зеркалом облегчает подстройку положения глаз для точного считывания, захватывая детальное изображение обоих глаз для обеспечения максимальной точности. Голосовые инструкции направляют положение пользователя для

Система распознавания по радужной оболочке глаза

Используется зафиксированное фокусирование, что позволяет ускорить процесс идентификации в отличие от систем с автоматической фокусировкой.

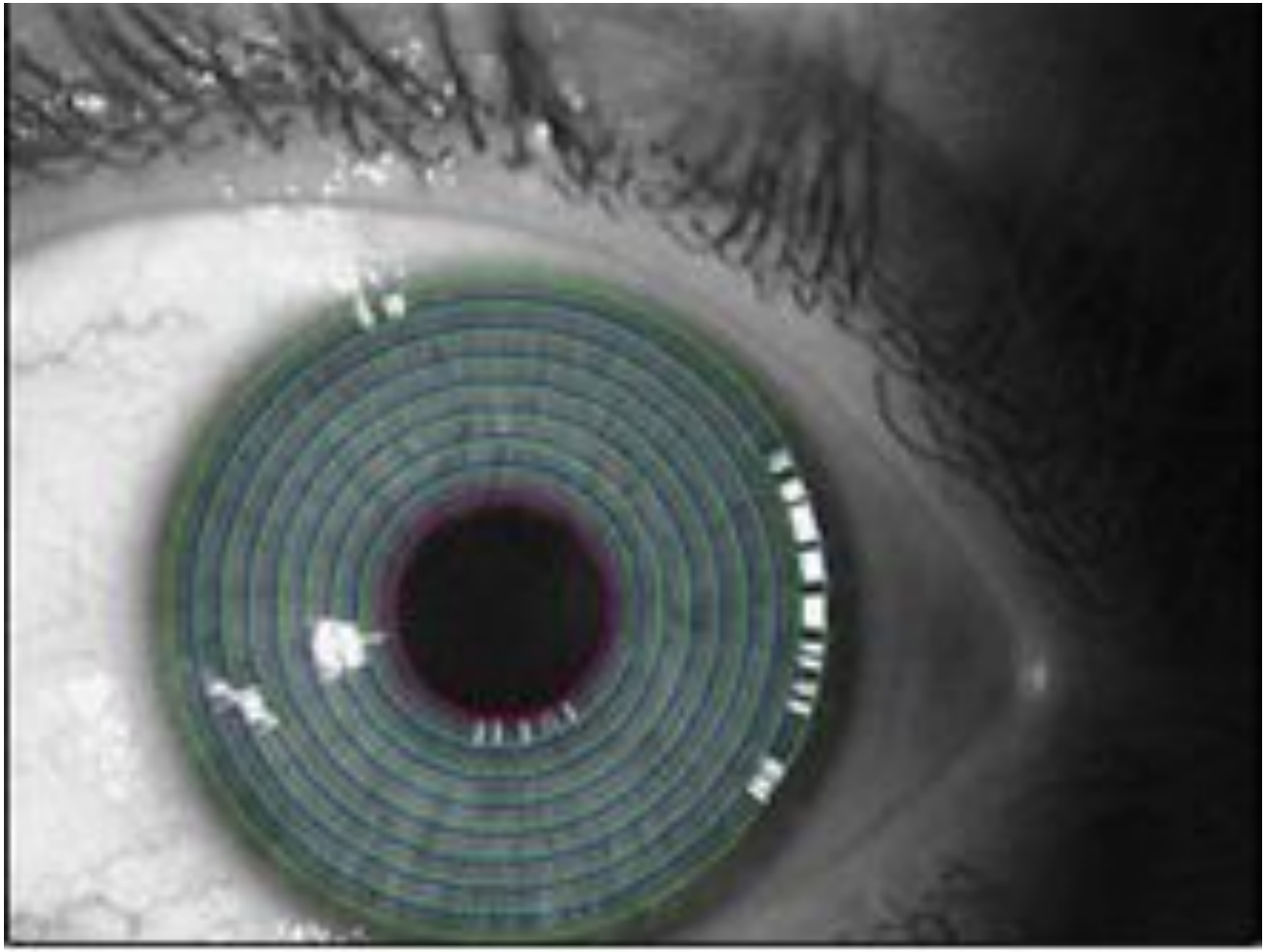
Аутентификация по сетчатке глаза

Сканирование сетчатки происходит с использованием инфракрасного света низкой интенсивности, направленного через зрачок к кровеносным сосудам на задней стенке глаза.

Особенности:

- один из самых низких процентов отказа в доступе зарегистрированным пользователям и почти нулевой процент ошибочного доступа;
- катаракта может отрицательно воздействовать на качество получаемого

Портативный сканер сетчатки глаза



Может поместиться, например, в мобильном телефоне.

Аутентификация по форме лица

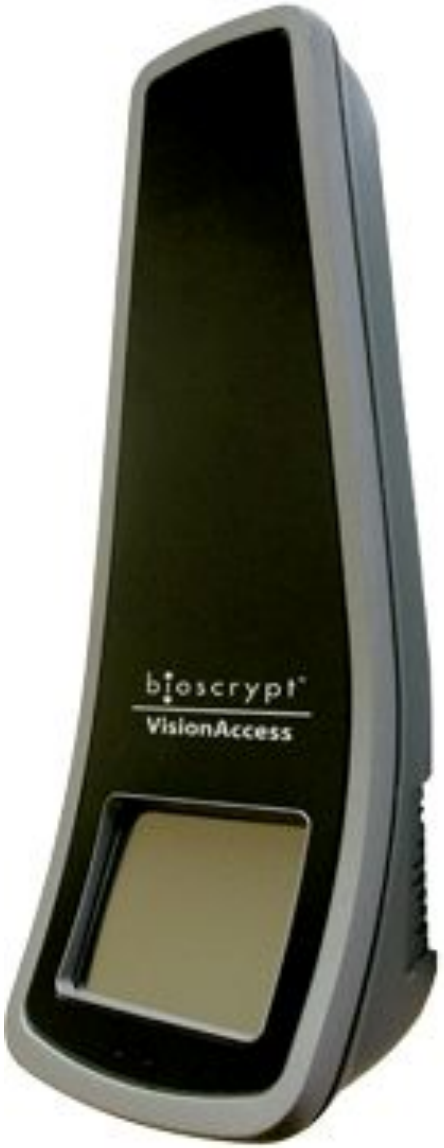
Способ основан на анализе большого количества параметров, таких как цвет, форма, контраст, черты и т.д.

Системы подобного рода в настоящее время имеют недостаточную надежность распознавания из-за большой чувствительности к освещенности и ракурсу лица во время ввода параметров идентификации.

Существует также проблема двойников (близнецов).

3D-сканер лица

Работает в инфракрасном диапазоне.



Мобильный телефон с камерой для аутентификации по лицу

Универсальный комплекс аутентификации

Системный блок компьютера,
оснащенный сканером
бумажных
документов,
видеокамерой-сканером лица
и
сканером отпечатков пальцев.

Другие статические биометрические характеристики

- Термограмма лица (схема расположения кровеносных сосудов лица). Используется специально разработанная инфракрасная камера.
- Фрагменты генетического кода (ДНК) - в настоящее время эти средства применяются редко по причине их сложности и высокой стоимости.

Термограмма лица, шеи и передней поверхности груди

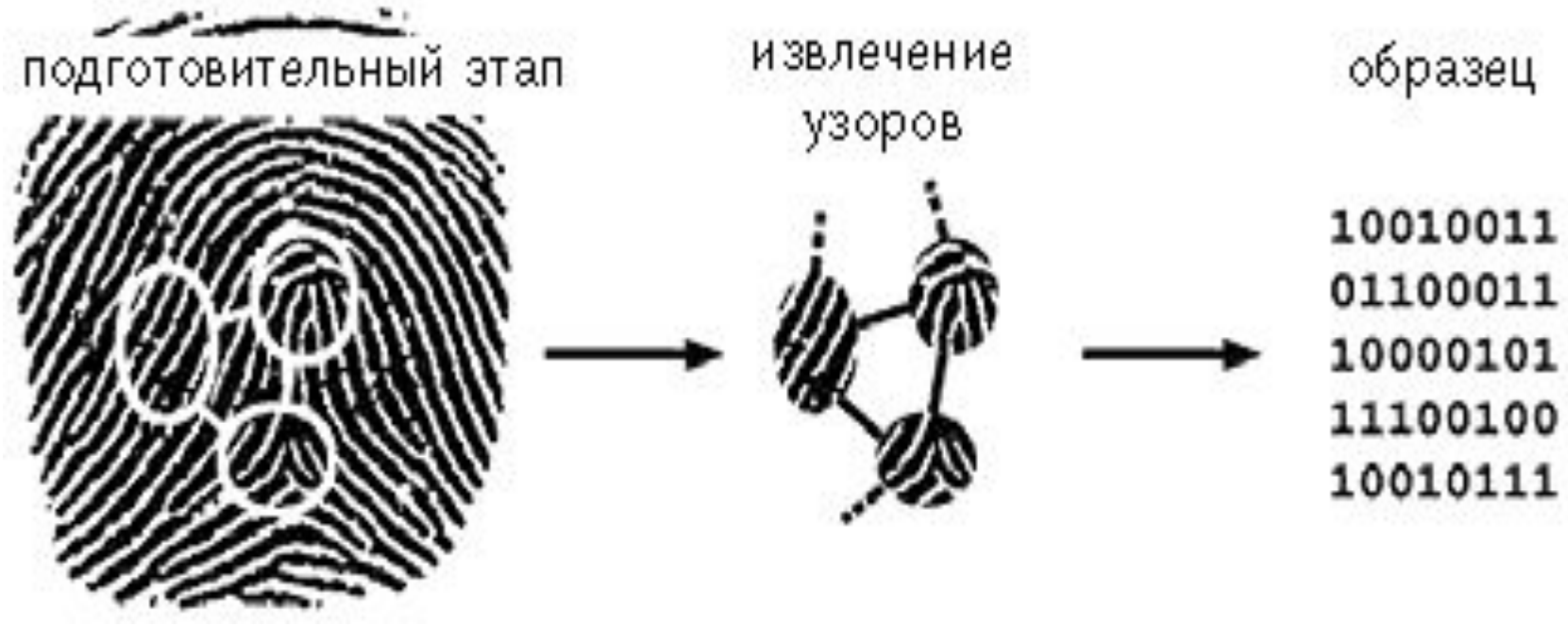
Динамические биометрические характеристики

- Голос.
- Рукописная подпись.
- Темп работы с клавиатурой (клавиатурный «почерк»).
- Темп работы с мышью («роспись» мышью).

Зависят от физического и психического состояния человека (в определенных случаях может являться преимуществом).

Порядок биометрической аутентификации

1. Снятие и преобразование в цифровую форму отличительной характеристики.



Оцифровка отпечатка пальца

Порядок биометрической аутентификации

2. Извлечение из считанной характеристики биометрической «подписи» проверяемого лица (например, пересечения и ветвления папиллярных линий на пальце и их взаимного расположения).

Порядок биометрической аутентификации

3. Поиск учетной записи, извлечение из нее биометрического эталона и сравнение его с полученной подписью.

Особенности биометрической идентификации и проверки уникальности

Имя пользователя может не запрашиваться, а полученная биометрическая подпись сравнивается с каждым эталоном в базе данных.

Создание биометрического эталона

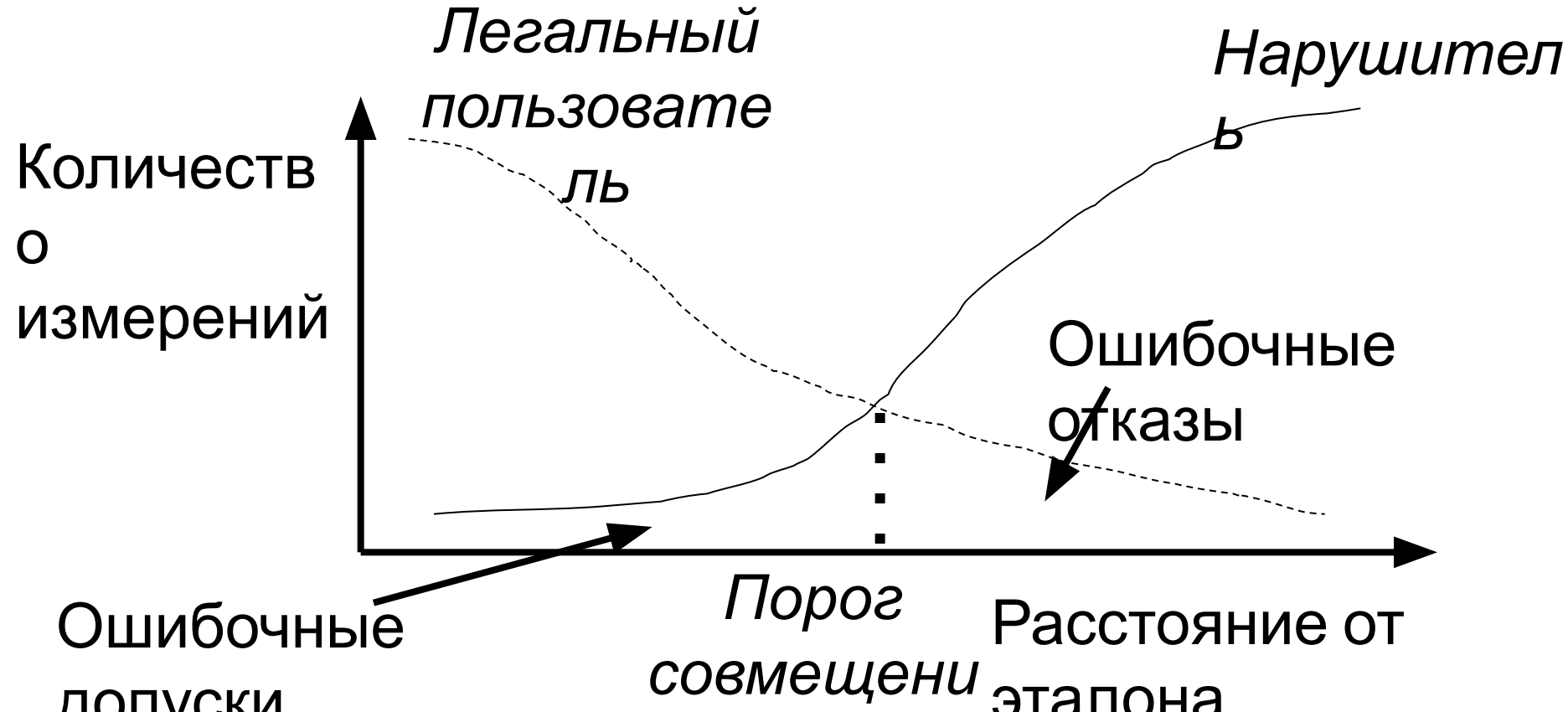
- Требуется достаточное количество измерений (для исключения естественных расхождений в измерениях и получения достоверного эталона).
- Возможно снятие нескольких подписей (например, отпечатков нескольких пальцев) для снижения риска ошибочного отказа.
- Иногда может потребоваться обучение пользователя, если снимаемая характеристика подвержена большим вариациям.

Проверка биометрической подписи

- В отличие от проверки паролей не требуется точное совпадение считанной биометрической подписи и эталона, сравниваются округленные значения.
- Для хранения биометрического эталона не может применяться хеширование.

Оценка точности биометрической аутентификации

Две оценки: вероятность ошибочного отказа (ошибки 1-го рода, FRR) и вероятность ошибочного допуска (ошибки 2-го рода, FAR).

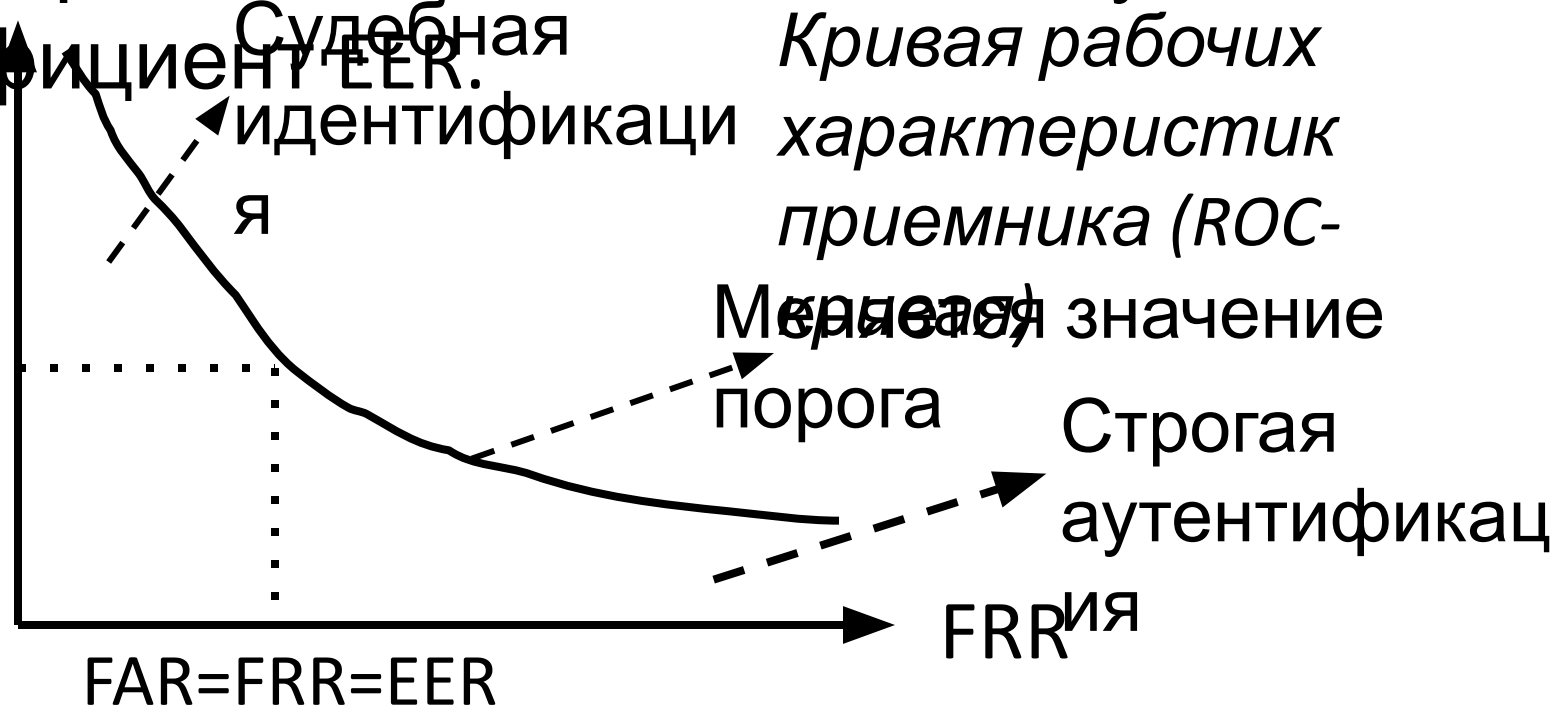


Настройка системы биометрической аутентификации

- Необходимо достижения компромисса между уровнем безопасности и удобством использования.
- Уменьшение порога допустимого отклонения от эталона снижает риск ошибочного допуска, но увеличивает риск ошибочного отказа.

Равная интенсивность ошибок

Т.к. FRR и FAR зависят от порога, для объективной оценки точности биометрической системы используется коэффициент EER.



Чем меньше EER, тем выше обеспечиваемый уровень безопасности.

Среднее пространство атаки для систем биометрической аутентификации

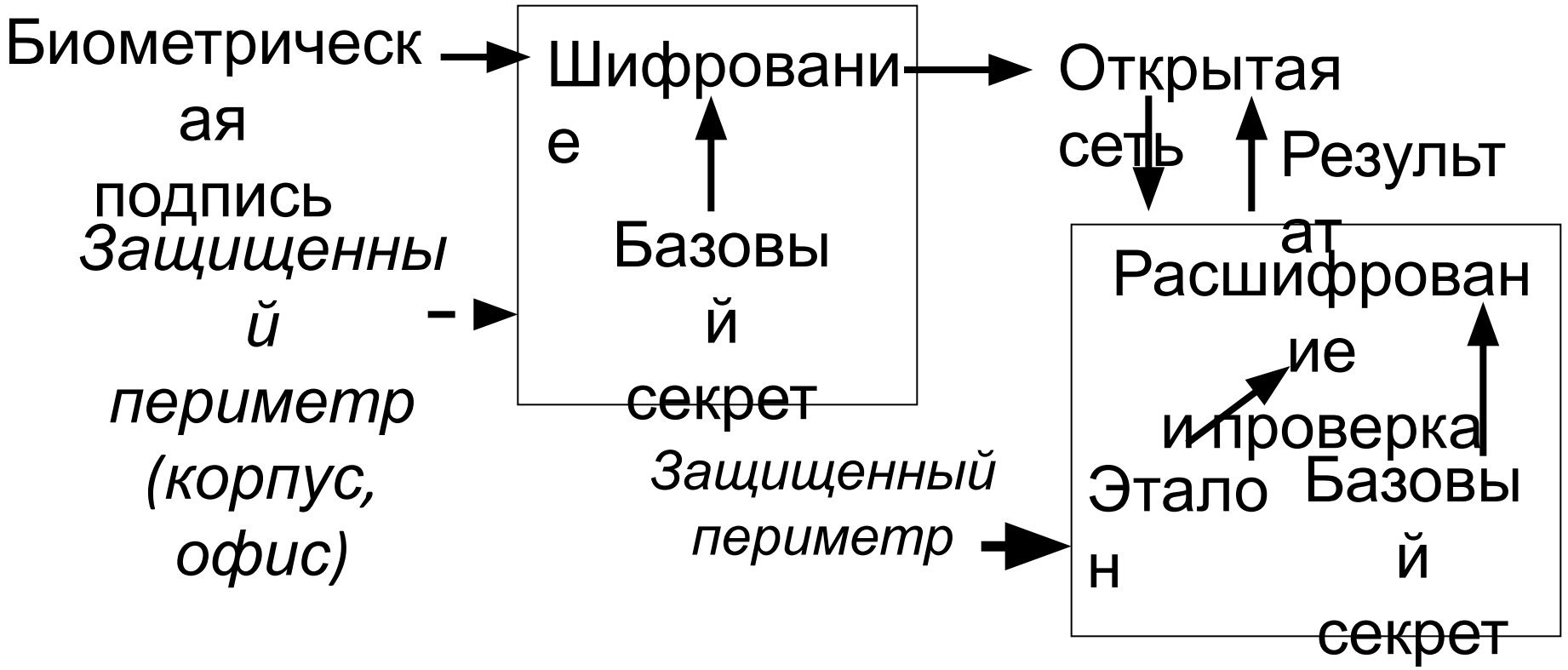
$\log_2(1/(2*FAR))$

Некоторые биометрические системы позволяют изменять значение порога и выбирать уровень безопасности, приемлемый для конкретной компьютерной системы.

Для $FAR=10^{-2}$, 10^{-5}, 10^{-6} имеем среднее пространство атаки 7, 16, 19 бит. Этого достаточно, т.к. возможны только попытки подбора в интерактивном режиме.

Использование криптографии в системах биометрической аутентификации

Обеспечение секретности пересылаемой биометрической информации.



Предотвращение угрозы перехвата эталона, построения подходящей подписи и ее отправки системе аутентификации

Обеспечение аутентичности биометрической характеристики:

- в устройство считывания добавляется базовый секрет;
- этот секрет используется совместно с хеш-функцией для получения кода аутентификации (хешируются биометрическая подпись, базовый секрет, идентификатор отправителя, отметка времени и/или случайный запрос).

Использование криптографии в биометрических системах

- Необходимость управления базовыми секретами снижает ценность биометрии в сетевых системах аутентификации.
- Это вполне приемлемо в системах определения уникальности (например, в протоколах голосования).

Обеспечение секретности биометрических данных

- Шифрование.
- Разграничение доступа.
- Передача биометрической системы под контроль консорциума заинтересованных сторон, ответственного за защиту тайны частной жизни пользователей, обеспечение надежности и эффективности работы системы (на основе принципов разделения полномочий и коллегиальности).