SCS SBERBANK CYBER SECURITY

Тенденции развития биометрической идентификации

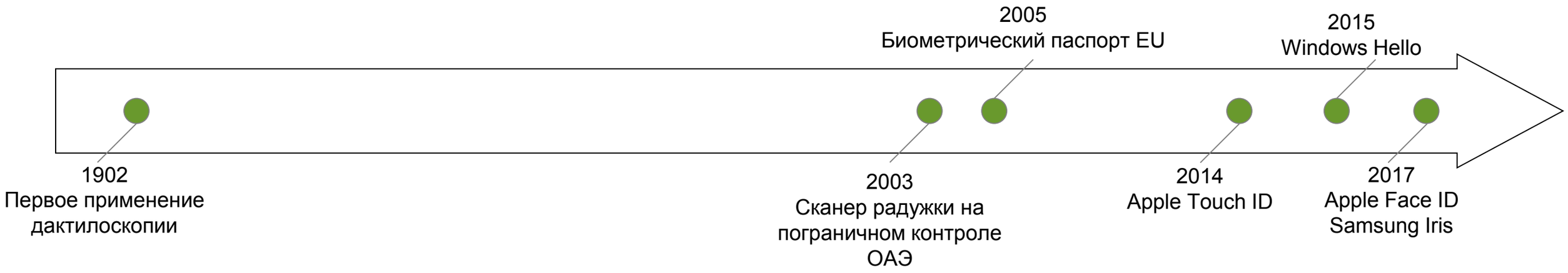
Антон Митрофанов

Москва, 2018

Содержание

- Как биометрия представлена в мире сейчас
- Что дают биометрические технологии бизнесу
- Недостатки биометрических технологий
- Безопасность биометрических технологий
- Риск-ориентированный подход к применению биометрии

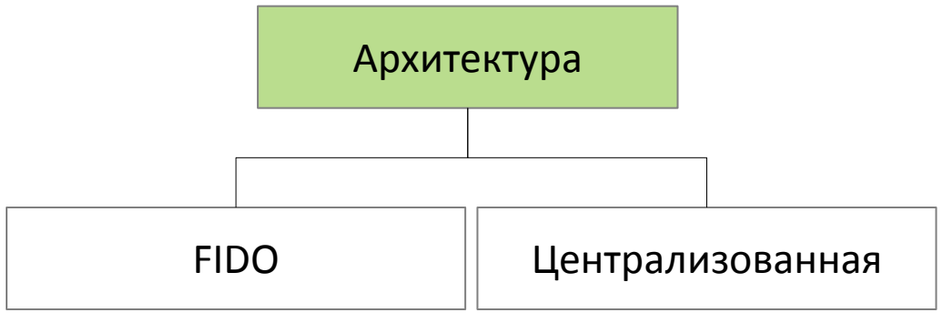
Развитие биометрии (1/2)
Технологии, примеры внедрений и массового использования

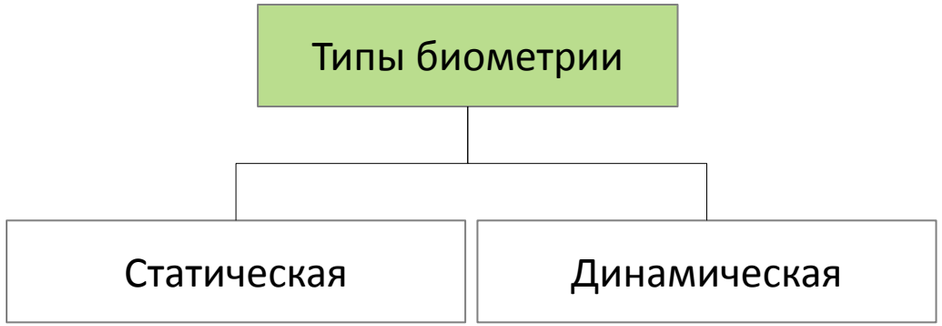


Как биометрия представлена сейчас

- Национальная биометрическая платформа в России
- Единая биометрическая база во Франции
- Система биометрических электронных документов в Индии
- Биометрический контроль в аэропортах по всему миру
- Персональные устройства с биометрическими сканерами
- Биометрические паспорта в различных странах
- Криминалистика по биометрическим признакам
- Умные очки китайской железнодорожной полиции

Развитие биометрии (2/2)
Подходы и технологии





Что дают биометрические технологии бизнесу и безопасности – почему они будут продолжать развиваться

Когда необходима идентификация в работе банка:

- обслуживание клиентов
- доступ сотрудников в помещения и информационные системы
- бизнес аналитика
- аналитика в целях обеспечения безопасности
- расследование инцидентов безопасности

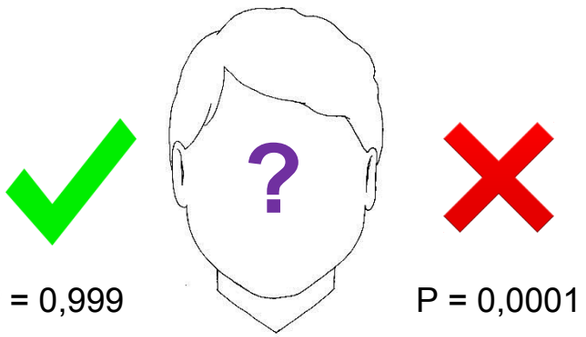
VS

В чем преимущество использования биометрии:

- Новый фактор обеспечения доверия
- Нельзя украсть, потерять, забыть – всегда доступен
- Повышает удобство использования сервисов
- Снижает операционные затраты на идентификацию
- Снизить риски мошенничества с поддельными документами

Недостатки биометрических технологий

Точность распознавания



P = 0,999

P = 0,0001

Вероятность ошибки при биометрической верификации всегда больше 0

Объемы поиска

?

Чем больше количество профилей - тем сложнее отличить одного человека от другого. Повышается вероятность ошибки ложного принятия

Живой человек или копия?

Применение биометрии для идентификации требует удостовериться что это действительно живой человек, а не попытка предъявить копию его биометрических данных.

Как сменить отпечатки пальцев или радужку?

Если по какой то причине сканер не может отличить копию от живого человека, то проблемой является смена скомпрометированных учетных данных

Если похищена база данных с биометрическими шаблонами – они все будут скомпрометированны

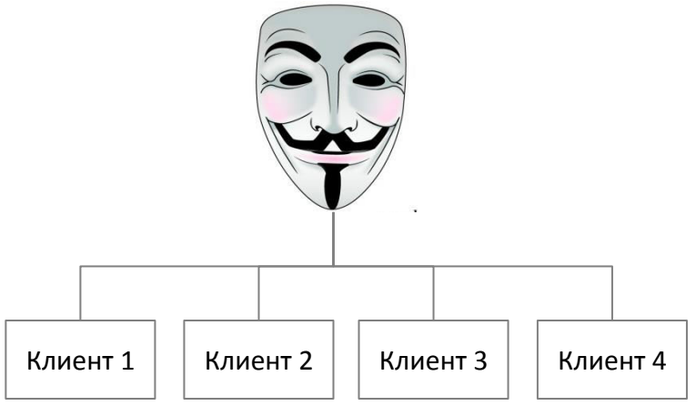
Атаки на сканер
Спуффинг

Возможности для копирования биометрических признаков растут с каждым днем. В 2008м году на расстоянии 6 метров был скопирован остаточный отпечаток пальца министра Германии, по которому был воссоздан силиконовый слепок.

Атаки на поисковый движок
Морфинг

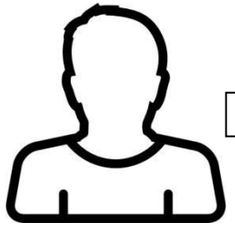
Если в систему распознавания заведена «не совсем ваша» биометрия, по которой может пройти кто то еще?
False Accept или злой умысел?

Атака на процессы
Кража личности

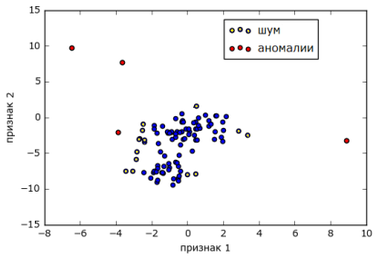


Если в базе данных шаблонов произошла «ошибка», и одно и то же лицо зарегистрированно у нескольких клиентов?

Риск-ориентированный подход к биометрической аутентификации(1/2)
Общие принципы использования. Мультимодальность.



1. Оценить уровень риска операции
2. Определить доступный пользователю состав challenge-а
3. Определить варианты достаточного состава challenge-а
4. Провести аутентификацию по выбранному набору факторов



- Оценка потенциального риска операции
- Использование поведенческого профиля для выявления аномалий
- Оценка уровня доверия к предъявленому образцу

- Определить доступные пользователю факторы (зарегистрированные)
- Определить ИТ окружение пользователя (наличие сканеров и возможность предъявить признак)

- На основании анализа риска операции определить необходимый и достаточный состав challenge-а
- Может сложиться ситуация что только биометрии недостаточно

- Запросить у пользователя выбранные факторы и модальности
- Подтвердить личность пользователя

Риск-ориентированный подход в применении биометрии (2/2)
Как измерить доверие к биометрическми шаблонам?

Канал регистрации биометрии в системе

При enroll-е образца в систему нужно учитывать откуда он был получен

Доверие к шаблонам, зарегистрированным по удаленным каналам существенно ниже чем при очном визите под контролем сотрудника

VS

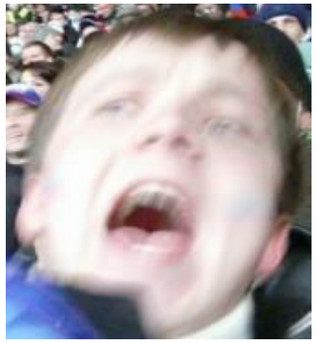
?

Качество исходного образца

Качество исходного образца, из которого извлечен шаблон, так же влияет на уровень доверия

Шаблоны, созданные из образцов низкого качества, сильно снижают точность распознавания, и повышают шанс ложного принятия

VS



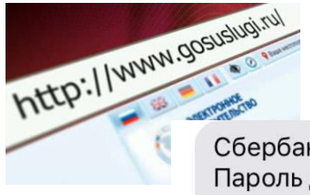
?

Подтверждение регистрации шаблона

Если рассматривать операцию регистрации биометрического шаблона как высокорисковую, то к ней так же можно применять риск-ориентированный подход

Шаблон, подтвержденный сильной комбинацией факторов, имеет более высокий уровень доверия

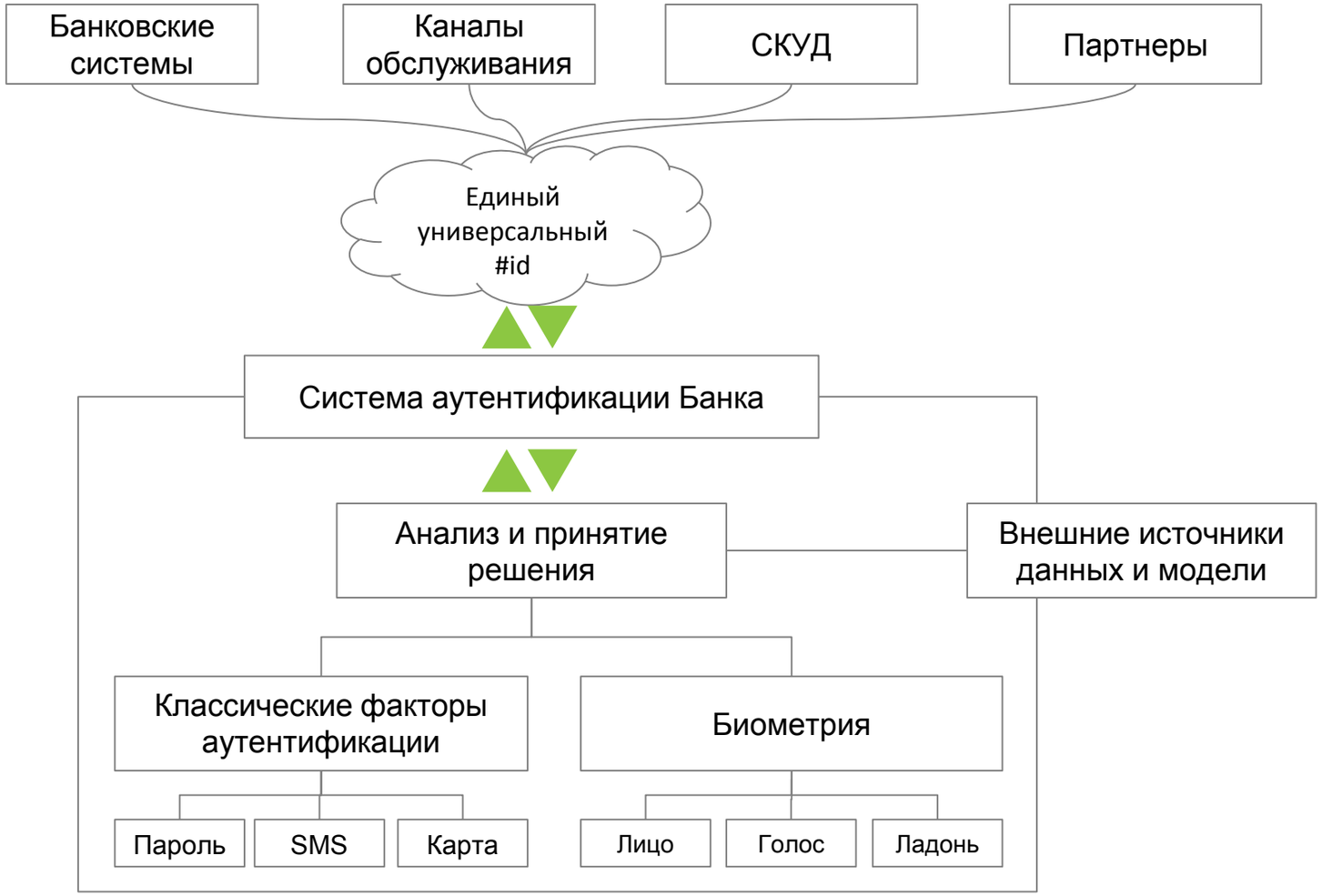
VS



Сбербанк Онлайн. Пароль для подтверждения входа в систему - 84770.

?

Единая система аутентификации



Ключевые принципы применения биометрии

- Риск-ориентированный подход к аутентификации
- Динамическое формирование challeng-а
- Комбинация с другими факторам аутентификации
- Использование нескольких модальностей

Что такое биометрия в этой системе

- Еще один способ повысить доверие к единому ID
- Один из факторов аутентификации, имеющий свои ограничения и недостатки
- Удобный инструмент, позволяющий клиентам минимизировать усилия для использования сервисов

Спасибо за внимание!

Вопросы?

ADMitrofanov@sberbank.ru

Все фото лиц взяты из открытых источников