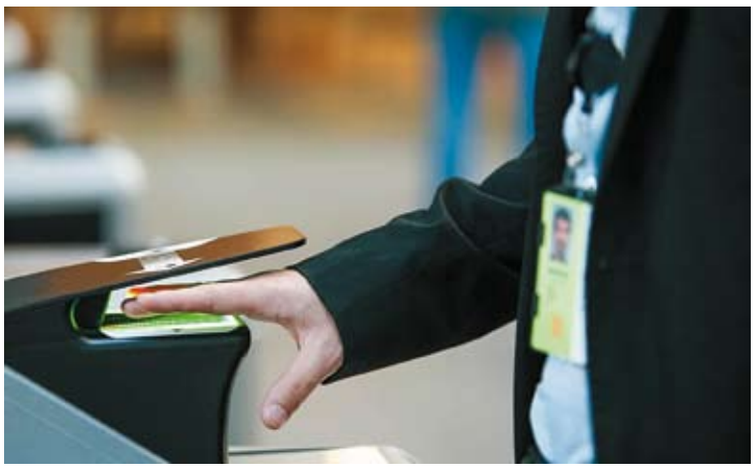
# Биометрические СКУД

**Василий МАМАЕВ, заместитель директора некоммерческого партнерства «Русское биометрическое общество»**



Основные определения, классификация и принципы испытаний СКУД изложены в ГОСТ Р 51241-2008 «Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний». Определения, касающиеся биометрических технологий целесообразно использовать из ГОСТ ISO/IEC 2382-37—2016 «Информационные технологии. Словарь. Часть 37. Биометрия». В данном стандарте установлены термины и определения в области биометрии, относящиеся к распознаванию человека, а также приведены в соответствие различные термины, используемые в действующих биометрических стандартах.

Некоторые основные определения

- Биометрическая характеристика (biometric characteristic). Биологические и поведенческие характеристики индивида, которые могут быть зарегистрированы и использованы в качестве отличительных, повторяющихся биометрических признаков для автоматического распознавания индивидов.

Примерами биометрических характеристик являются: папиллярная структура Гальтона, топография лица, текстура кожи лица, топография кисти руки, топография пальца, структура радужной оболочки глаза, структура сосудов кисти руки, папиллярная структура ладони, изображение сетчатки глаза, динамика рукописной подписи и голос.

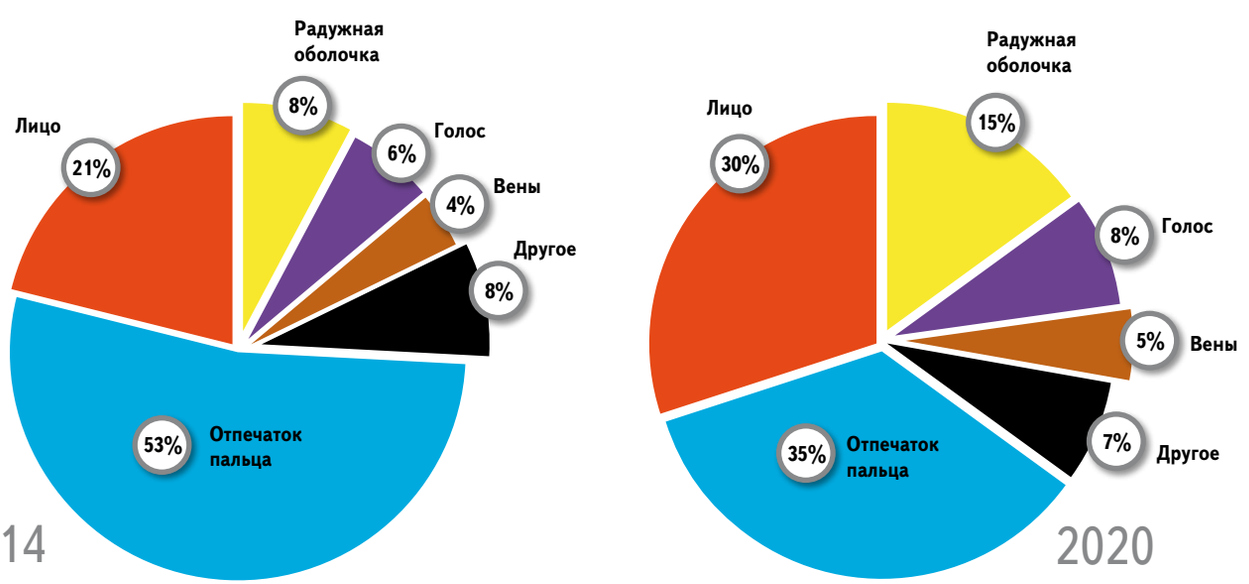
- Биометрическое распознавание (biometric recognition)/биометрия (biometrics). Автоматическое распознавание индивидов, основанное на их поведенческих и биологических характеристиках.
- Аутентификация (authentication). Действие, доказывающее или показывающее бесспорное происхождение или достоверность.
- Биометрическая идентификация (biometric identification). Процесс поиска по базе данных биометрических регистраций, направленный на поиск и возврат идентификатора(ов) биометрического контрольного шаблона, связанного с одним индивидом.
- Биометрическая верификация (biometric verification). Процесс подтверждения биометрического заявления при сравнении.

В 2016 году Techportal.ru опубликовал прогноз развития структуры биометрических идентификационных признаков на 2020 год по сравнению с 2014 годом.

На мой взгляд, на сегодняшний день развитие в большей степени получили биометрические технологии распознавания по венам ладоней и пальцев, а также технологии радужной оболочки глаза. Причина развития данных технологий, прежде всего в их преимуществах — бесконтактном способе считывания и практической невозможности подделок.

Однако данный прогноз не учитывает развитие по потребительским секторам. В настоящее время абсолютное большинство применений СКУД — это промышленные и государственные учреждения, в том числе предприятия, где требуется повышенные меры безопасности. Сюда также относятся и учреждения здравоохранения и образования и спортивные комплексы. Внедрение

Мировой рынок биометрических технологий. Динамика развития. Прогноз до 2020 г.



СКУД в гражданский сектор (квартиры, коттеджи) не получило широкого распространения, все мы привыкли пользоваться обычными ключами и считаем это достаточно надежным методом защиты своего дома.

Однако достижения биометрии позволяют сделать вывод о том, что эффективность биометрических решений, выраженная через современные биометрические технологии, достаточна велика и позволяет обеспечить надежную защиту.

Несомненным преимуществом биометрических СКУД, а для граждан это биометрический замок, является отсутствие необходимости носить с собой ключи, которые также могут похитить.

Биометрические СКУД для жилья граждан внедряются достаточно медленно, однако данный рынок является, на мой взгляд, наиболее емким в настоявший момент. Сдерживающим фактором для широкого использования биометрических замков является их стоимость, относительная непривычность применения и отсутствие доверия у потребителей. В этом секторе наиболее интересными для развития будут являться технологии распознавания по венам ладоней и пальцев.

Следующим потребительским сектором, в котором происходит развитие и будет расширяться применение, является сектор автоматических пропускных устройств на транспортных узлах: в аэропортах, автовокзалах, железнодорожном транспорте.

Говоря о путях дальнейшего развития систем СКУД следует также отметить использование многофакторной биометрии.

В последнее время в области биометрических технологий начала также развиваться поведенческая биометрия, однако в области СКУД она вряд ли в будущем будет использоваться.

В обзоре Technoportal.ru был приведен перечень фирм, бренды которых наиболее узнаваемы (рисунок 1).

Далее рассмотрены только считыватели, то есть автономные устройства, которые можно использовать без дополнительных контроллеров. Конечно, при построении комплексной системы СКУД на предприятии потребуется наличие мощного центра обработки и контроля считывателей СКУД и систем охраны всех помещений.

Можно сделать вывод, что рынок биометрических считывателей в настоящий момент достаточно широк, даже в развивающихся направлениях – вены, радужная оболочка глаза – можно найти разнообразные примеры устройств. Причем цена данных изделий может быть весьма приемлема для оборудования жилья.

Возникает простой вопрос: как правильно выбрать необходимый биометрический СКУД?

Наиболее значимой характеристикой биометрических изделий являются показатели ошибок первого и второго рода.

В статье [1] приведен известный график соотношения ошибок первого (FRR- непропуск хозяина) и второго (FAR – пропуск нарушителя) рода, который показывает, что любая биометрическая система может быть так настроена, что ошибки первого рода будут крайне малы, а второго – значительны и наоборот. Такая настройка часто выполняется разработчиками и/или настройщиками биометрических СКУД, что вполне законно позволяет получить надежную работу при пропуске хозяина и непропуске нарушителя.

FRR (false reject rate) или вероятность ложного недопуска ВЛНД – доля транзакций верификации подлинного лица, которые будут ошибочно отвергнуты.

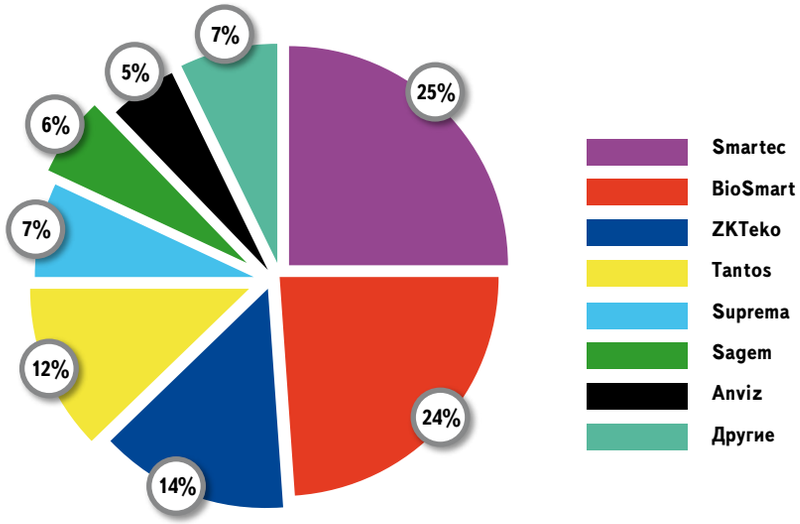



**Рисунок 1. Перечень наиболее узнаваемых брендов**

FAR (false accept rate) или вероятность ложного допуска ВЛД – доля транзакций верификации «самозванца», которые будут ошибочно приняты.

Дело здесь заключается в том, что не все производители при описании своих систем дают соотношения ошибок первого и второго рода.

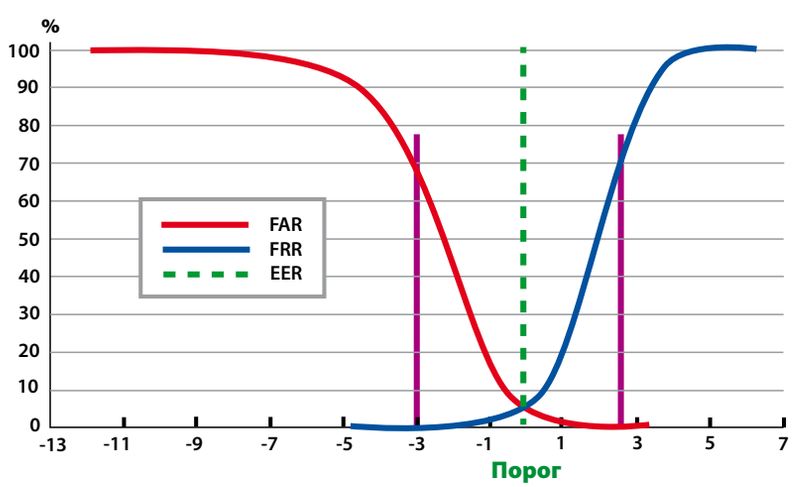
Но – и это самое главное – для того, чтобы оценить эти ошибки, необходимо проводить достоверные и трудоемкие испытания согласно комплексу биометрических ГОСТ.

Низкая воспроизводимость результатов биометрической идентификации обусловлена разнообразием аппаратных и программных решений для каждой биометрической технологии, а также высокой вариабельностью биометрических характеристик человека, связанной с нестабильностью условий регистрации (например, неправильное положение головы и неравномерное освещение при регистрации изображения лица или изменение диаметра зрачка в зависимости от освещенности при регистрации изображений радужной оболочки глаза).

Для унификации условий регистрации и обеспечения взаимозаменяемости технических частей биометрических систем разработан комплекс национальных стандартов [2]:

- ГОСТ Р ИСО/МЭК 19795-1–2007 «Автоматическая идентификация. Идентификация биометрическая. Эксплуатационные испытания и протоколы испытаний в биометрии. Часть 1. Принципы и структура». В стандарте установлены общие требования к проведению эксплуатационных испытаний биометрических систем, эксплуатационные характеристики, а также требования к записи данных и представлению результатов испытаний.

## График соотношения ошибок первого (FRR- непропуск хозяина) и второго (FAR – пропуск нарушителя) рода



- ГОСТ Р ИСО/МЭК 19795-2—2008 «Автоматическая идентификация. Идентификация биометрическая. Эксплуатационные испытания и протоколы испытаний в биометрии. Часть 2. Методы проведения технологического и сценарного испытаний». В стандарте установлены общие требования к разработке, проведению и представлению результатов двух основных видов эксплуатационных испытаний биометрических систем — технологического и сценарного.
- ГОСТ Р ИСО/МЭК ТО 19795-3—2009 «Автоматическая идентификация. Идентификация биометрическая. Эксплуатационные испытания и протоколы испытаний в биометрии. Часть 3. Особенности проведения испытаний при различных биометрических модальностях». Стандарт предназначен для использования при разработке методов проведения испытаний биометрических систем с различными биометрическими модальностями. В стандарте приведены рекомендации по разработке испытаний с целью определения технических и эксплуатационных характеристик биометрических систем с учетом особенностей биометрической модальности.
- ГОСТ Р ИСО/МЭК 19795-4—2011 «Информационные технологии. Биометрия. Эксплуатационные испытания и протоколы испытаний в биометрии. Часть 4. Испытания на совместимость». В стандарте установлены общие требования к проведению испытаний для оценки степеней совместимости и достаточности, а также абсолютных и относительных эксплуатационных характеристик разнородных биометрических систем, использующих соответствующие утвержденным стандартам (в частности, стандартам ИСО/МЭК 19794) форматы обмена биометрическими данными.
- ГОСТ Р ИСО/МЭК 19795-6—2015 «Информационные технологии. Биометрия. Эксплуатационные испытания и протоколы испытаний в биометрии. Часть 6. Методология проведения оперативных испытаний». В стандарте установлены общие требования к разработке, проведению и представлению результатов оперативных испытаний. Оперативное испытание отличается от технологического и сценарного испытаний тем, что база субъектов, внешние условия и конструкция биометрической системы больше не контролируются с целью реализации воспроизводимых испытаний, а изменяются в соответствии с использованием биометрической системы в рабочем режиме.

В соответствии с ГОСТ различают следующие виды испытаний:
- Технологическое испытание (technology evaluation). Испытание одного или более алгоритмов распознавания одинаковых биометрических модальностей с использованием существовавшей ранее или специально собранной базы данных образцов в режиме отложенного задания.
- Сценарное испытание (scenario evaluation). Испытание, при проведении которого эксплуатационные характеристики системы определяются с помощью прототипа или имитирующего приложения.
- Оперативное испытание (operalional evaluation). Испытание, в котором эксплуатационные характеристики биометрической системы определяются в специальных условиях эксплуатации по специальной целевой выборке.
- Режим реального времени (online). Режим испытания, при котором регистрация и сравнение выполняются в процессе представления изображения или сигнала.
- Режим отложенного задания (offline). Режим испытания, при котором регистрация и сравнение выполняются отдельно от процесса представления изображения или сигнала.

Стандарты, касающиеся проведения испытаний, обеспечивает возможность:
- проведения достоверных и корректных испытаний биометрического оборудования и алгоритмов, в том числе, правильное проведение различных видов испытаний (технологическое, сценарное, оперативное);
- единообразное оформление протоколов испытаний;
- проведение испытаний различных алгоритмов в одинаковых условиях;
- использование проверочных баз данных, не зависящих от разработчиков;
- проведение корректных испытаний методов определения подделок/муляжей (liveness detection).

Крупные производители, давно работающие на рынке, имеют возможность проводить полномасштабные самостоятельные испытания и участвовать в испытаниях, которые проводят зарубежные центры. Отечественные фирмы — «Сонда», «Папилон» заняли лидирующие места в таких испытаниях как Fingerprint Vendor

Technology Evaluation (NIST, 2012) и FVC-onGoing (FVC, 2018), на которых проводились технологические испытания алгоритмов распознавания отпечатков пальцев.

Сценарные и оперативные испытания, позволяющие определить работоспособность системы в условиях, близких к реальным, фирмы проводят самостоятельно.

Типовые ошибки при проведении испытаний:

- незнание (непонимание) основных видов испытаний;
- использование БД с биометрическими образцами из открытых источников;
- формирование испытуемой группы из представителей заказчика и разработчика;
- некорректное определение размера испытуемой группы;
- увеличение числа испытаний путем увеличения числа транзакций для одного субъекта;
- отсутствие попыток «активного» и «пассивного» самозванца при проведении испытания;
- испытание различных биометрических алгоритмов и систем в неодинаковых условиях, что приводит к искажениям результатов и получению недостоверных значений ошибок первого и второго рода.

В этих условиях, когда испытания проводятся фирмами по непонятным потребителю критериям, возникает проблема выбора надежной системы СКУД.

Воспользуемся советами одного из экспертов рынка К.А. Новикова [3]:

«Во-первых, поставьте четкую задачу – для чего вам нужна биометрическая система, какие функции она должна выполнять.

Во-вторых, при выборе любой биометрической системы узнавайте величину FAR/FRR.

В-третьих, проконсультируйтесь с профессионалами о характеристиках системы:

- температурный режим;
- гарантия;
- возможности программного обеспечения – если они есть;
- параметры безопасности – возможность обмана системы, манипуляции извне, варианты расположения управляющих элементов и доступа к ним;
- время распознавания;
- возможность наращивания системы или ее модернизации.»

Относительно стандартов хотелось бы также отметить, что касательно биометрических СКУД в ГОСТ Р 51241-2008 указано, что «5.2.2.5 Биометрические считыватели, при их применении в СКУД, должны соответствовать требованиям ГОСТ Р ИСО/МЭК 19794-2, ГОСТ Р ИСО/МЭК 19794-4, ГОСТ Р ИСО/МЭК 19794-5, ГОСТ Р ИСО/МЭК 19794-6.» Эти ГОСТ касаются такой важной темы как унификация форматов обмена биометрическими данными, что необходимо учитывать при построении биометрических государственных систем.

**Литература**

[1] https://algoritm.org
Основные параметры биометрических систем
Михайлов А. А. Колосков А.А. Дронов Ю.И.
[2] http://www.allbiometrics.ru
[3] file:///E:/статья%20для%20Технол%20защиты/Информация/_%20Secuteck.Ru.html