Место биометрии в иерархии доверия к идентификации и аутентификации

16 февраля 2017 г.

Алексей Сабанов, к.т.н.,
ЗАО "Аладдин Р.Д."

Технологии ИА

Определения

Идентификация – действия по присвоению субъектам и объектам доступа идентификаторов и (или) по сравнению предъявляемого идентификатора с перечнем присвоенных идентификаторов. **Идентификаторы**: совокупность атрибутов, связанных с конкретным субъектом (объектом) доступа. **Атрибут**: характеристика или свойство субъекта или объекта доступа.
Аутентификация – процесс, состоящий из процедур, включающих подтверждение подлинности предъявленного претендентом (субъектом доступа) идентификатора и проверку принадлежности аутентификационной информации и идентификатора конкретному субъекту или объекту доступа.
Факторы аутентификации:
- что-то, что субъект знает, например, пароль, ПИН-код и т. п.;
- что-то, чем субъект или объект обладает, например, данные, хранимые в аппаратных средствах аутентификации;
- что-то, что свойственно субъекту, например, биометрические данные физического лица и (или) поведенческие характеристики.

Виды идентификации

Идентификация включает первичную идентификацию, проводимую в момент регистрации нового субъекта доступа в ИС, и вторичную идентификацию (регулярно повторяющуюся), выполняемую при каждом новом запросе на доступ.

Первичная идентификация субъекта доступа может являться одновременно частью как процесса идентификации, так и процесса аутентификации (если используется процесс аутентификации).

Требования к первичной идентификации при применении процесса аутентификации строже, чем при идентификации, не предполагающей последующего применения процесса аутентификации (например, получение уникального идентификатора в государственном реестре или регистре).

Первичная идентификация

Целью первичной идентификации является обеспечение отсутствия коллизий представленной заявителем для целей включения в состав пользователем ИС от другой (принадлежащих другим пользователям данной ИС) идентификационной информации (ИИ), имеющейся в данной ИС.

Полнота и строгость проверки представленной заявителем ИИ определяется политикой безопасности оператора ИС. Проверка может проводиться как в ручном, так и автоматизированном режиме в соответствии с установленным оператором ИС или обладателем информации порядком.

Первичная идентификация должна завершаться регистрацией (присвоением новому пользователю уникального идентификатора в данной ИС) или обоснованным отказом. Причиной отказа может являться недостаточный объем представленной ИИ. Объём связанной с новым пользователем необходимой ИИ определяется политикой безопасности оператора ИС.

Первичная идентификация должна определять возможность регистрации данного субъекта или объекта в конкретной ИС.

Вторичная идентификация

Целью вторичной идентификации должна являться проверка соответствия (верификация) предъявленного претендентом идентификатора занесённому ранее в базу данных ИС. При совпадении предъявленного и зарегистрированного в ИС идентификаторов процесс идентификации должен считаться успешно пройденным, а система управления доступом должна передать дальнейшее управление в систему аутентификации.

Процесс вторичной идентификации должен проводиться в автоматическом режиме.

Идентификация должна осуществляться в границах одной ИС (области применения политики безопасности ИС) или границах нескольких ИС при условии распространения на них единой политики безопасности.

Биометрическая идентификация, как правило, используется в качестве дополнительного фактора в доказательстве владения пользователем идентификационной и аутентификационной информации .

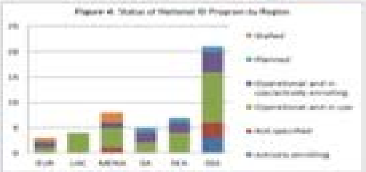
Модная тема: биометрическая идентификация

В 2017 году с участием банков из ТОП-50 планируются пилот создаваемой ЦБ единой базы биометрических данных россиян
http://www.rbc.ru/finances/19/01/2017/587e2c689a79470b502835ba?from=newsfeed
ВТБ: денежные переводы через мобильное приложение банка с использованием сканера отпечатка пальа смартфона www.cnews.ru/top/2017-01

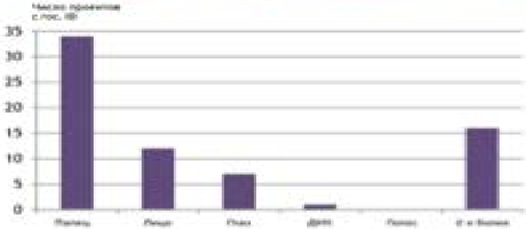
ВТБ-24: Биометрическая идентификация по видео и голосу для интернет-банкинга; Голосовая идентификация клиентов, звонящих в Call-центр
Тинькофф – банк: идентификация по голосу, идентификация по лицу

Банк «Открытие» запустил идентификацию клиентов с использованием системы по анализу биометрии лица
Источник:
https://bosfera.com/press-release/bank-otkrytie-vnedril-sistemu-raspoznavaniya-lic

Тем временем в мире…



Страна	Официальное название национального ID	[illegible]	[illegible]	Личная информация				Биометрическая информация					[illegible]
				[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	
Афганистан	e-tazkira	Да	Да	Да	Да	Да	Да	Да	Нет	Да	Нет	Нет	Да
Алжир	National ID	Да	Да	Да		Да	Да	Нет	Нет	Нет	Нет	Нет	
Ангола	National ID	Да	Да					Да	Нет	Да	Нет	Нет	Да
Бангладеш	National Identity Card (NID)	Да	Да	Да		Да	Да	Да	Нет	Нет	Нет	Нет	Да
Буркина-Фасо	National ID	Да											
Камбоджа	National ID	Да	Да	Да	Да	Да	Нет	Да	Нет	Нет	Нет	Нет	Да
Камбоджа	IDPoor	Да		Да	Да								Да
Камерун	National Identity Card	Да	Нет	Да	Да	Да	Да	Да	Нет	Нет	Нет	Нет	Да
Китай	Second Generation Resident Identity Card	Да	Да	Да	Да	Да	Да	Да	Нет	Нет	Нет	Нет	Да
Колумбия	Registraduria Nacional del Estado Civil	Да		Да	Да	Да	Да	Да	Нет	Нет	Нет	Нет	Да
Конго	Elector's Card	Да	Да	Да	Да	Да	Да	Да	Нет	Нет	Нет	Нет	Да
Кот д'Ивуар	National ID	Да						Да	Нет	Нет	Нет	Нет	Да
Эквадор	Cedula de Identidad	Да	Да	Да	Да	Да	Да	Да	Да	Нет	Нет	Нет	
Эфиопия	Regional ID	Да	Нет	Да	Да	Да	Да						Да
Гана	GhanaCard	Да	Да	Да	Да	Да	Да	Нет	Да	Нет	Нет	Нет	Да
Гватемала	Documento Personal de Identificación (DPI)	Да	Да	Да	Да	Да	Да	Да	Да	Нет	Нет	Нет	Да



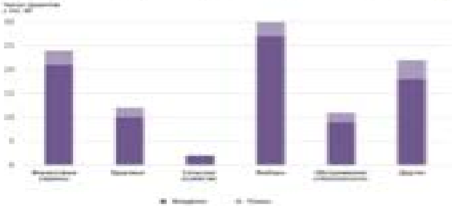
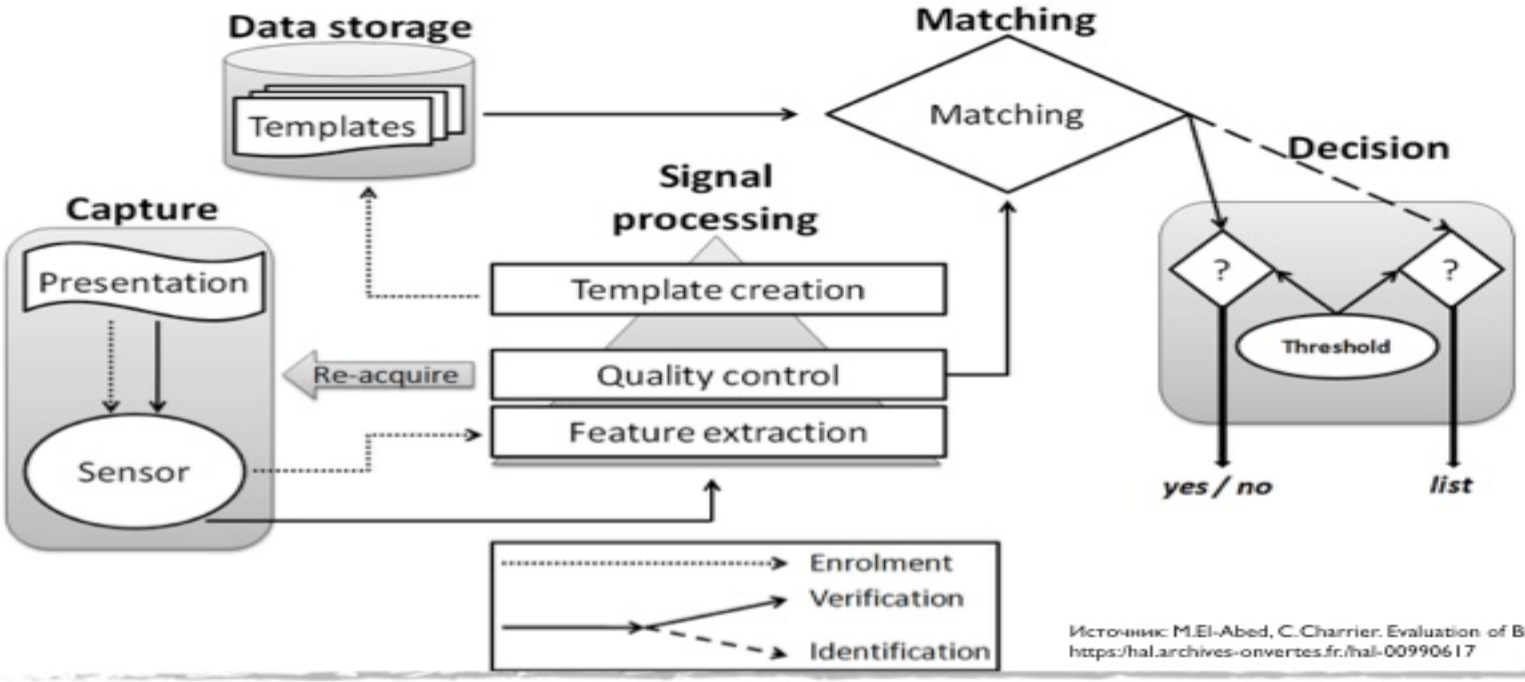


Figure 8. Financial Connections to ID Programs

Источник: NIST FG-DFS 05/2016

Состав биометической системы



Источник: M.El-Abed, C.Charrier. Evaluation of Biometric Systems
https://hal.archives-ouvertes.fr/hal-00990617

Анализ биометрической системы

Качество данных

•Необходимы единые требования и регламенты сбора эталонных и предъявляемых данных – ошибка в эталонах возрастает многократно при сравнении с предъявленными характеристиками

•Пользователь предъявляет биохарактеристики в "полевых условиях" – неизбежны отличия от образцов, полученных в офисе банка (эталонов)

•Математические методы поиска и сравнения биометрических характеристик и их электронных образов

Удобство для пользователей

Безопасность

•Угрозы и уязвимости – основные имеются в ISO/IEC 19792, ISO 15408: 2013.

•Защищенность базы данных эталонных биометрических характеристик граждан: любая успешная атака на базу приводит к фатальному исходу – требования к конфиденциальности и разделению доступа при одновременном жёстком требовании доступности

•Разница между применением биометрических методов на контролируемой территории и в "полевых" условиях (грязь, плохая освещенность, углы поворота), где могут подсунуть муляж

•Кроме специфических для систем биометрии, необходимо учитывать все атаки, характерные для любой ИС.

Источник: M.El-Abed, C.Charrier. Evaluation of Biometric Systems https://hal.archives-ouvertes.fr/hal-00990617

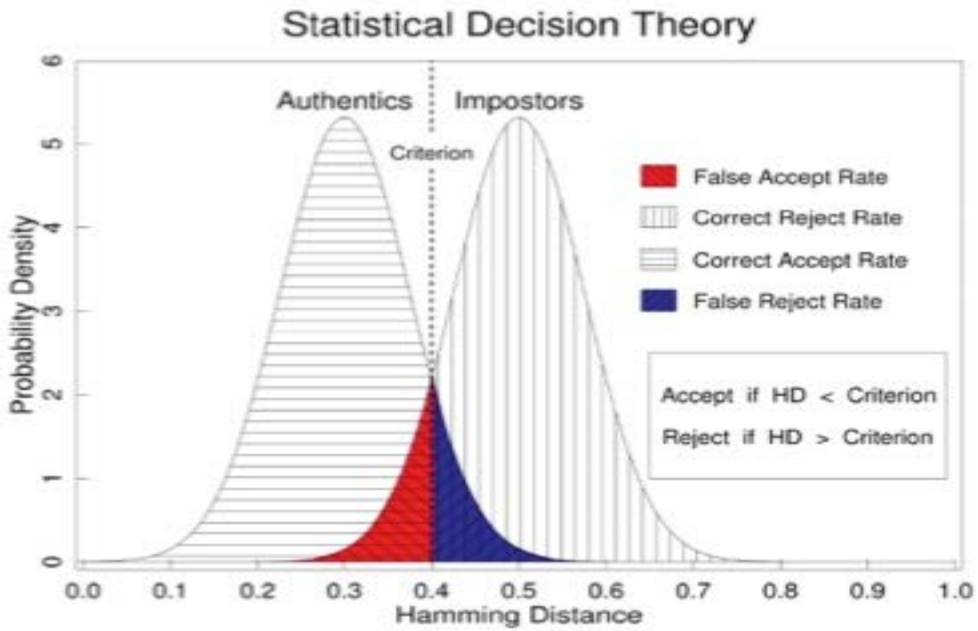
Сравнение биометрических методов

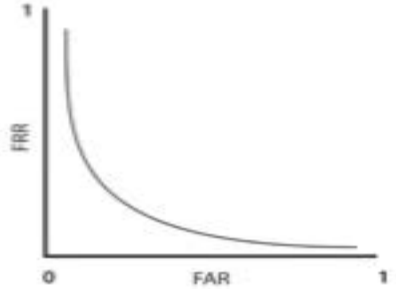
Идентификатор/ критерий	Универсальность	Однозначность	Устойчивость	Простота сбора данных	Производительность	Удобство пользования	Простота обмана
ДНК	В	В	В	Н	В	Н	Н
Ухо	С	С	В	С	С	В	С
Лицо	В	Н	С	В	Н	В	В
Палец	С	В	В	С	В	С	С
Геометрия руки	С	С	С	В	С	С	С
Вены руки	С	С	С	С	С	С	Н
Радужка	В	В	В	С	В	Н	Н
Сетчатка глаза	В	В	С	Н	В	Н	Н
Голос	С	Н	Н	С	Н	В	В

обозн.цвета:
- преимущество
- недостаток
- средне

Источник: A.Clocova. Comparison of Various Biometric Methods. University of Southhampton, UK. 2014.

Биометрия: ошибки I и II рода



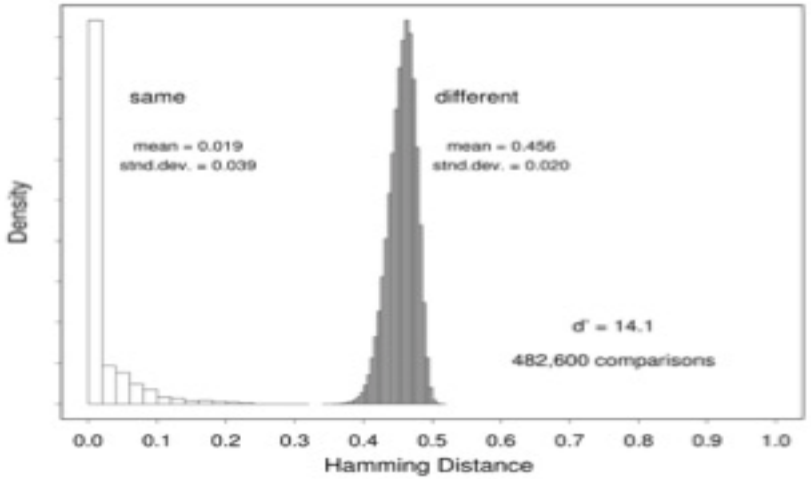


Это – теория.

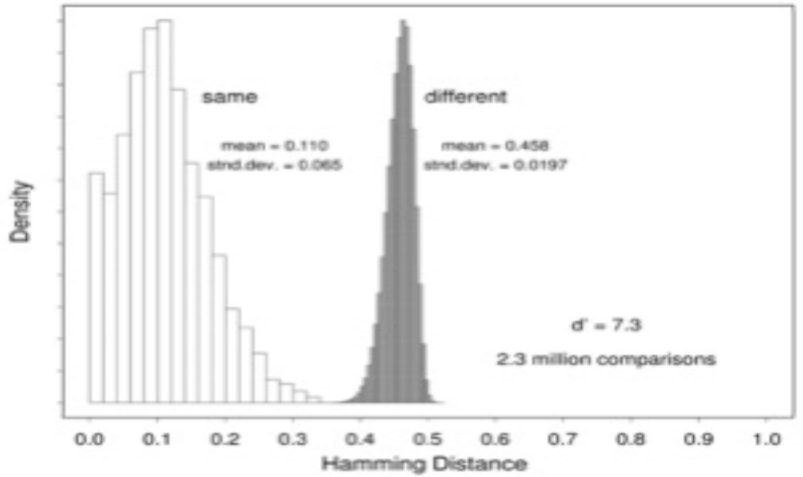
На практике всё немного не так.

Источник: John Daugman. Recording Persons by their Iris Pattern. University of Cambridge. 2014.

Биометрия: исследования радужки



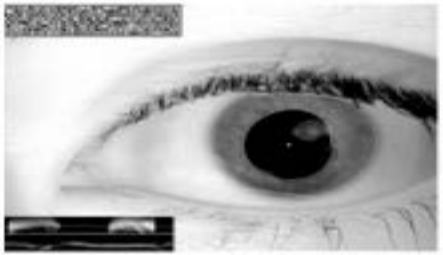
Идеальные изображения



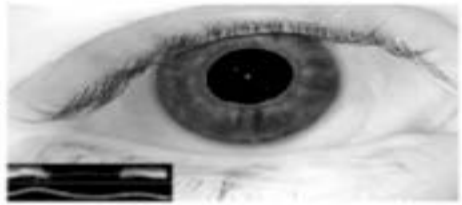
Из практики

Источник: John Daugman. Recording Persons by their Iris Pattern. University of Cambridge. 2014.

Биометрия: Радужная оболочка



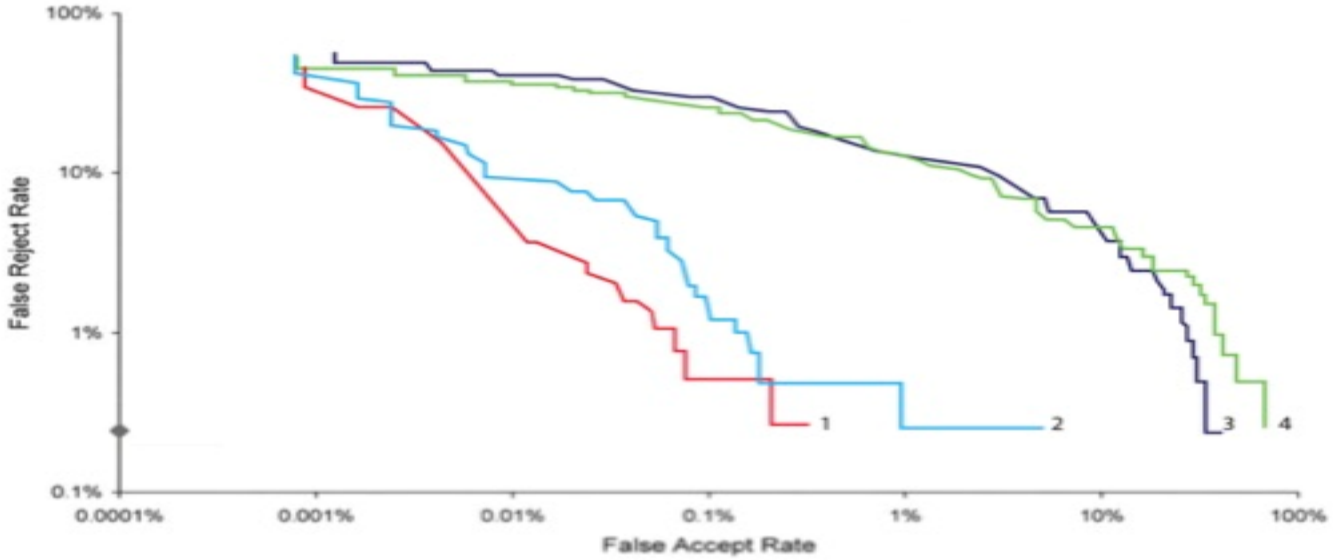
Общее число Бит	Процент видимости радужной оболочки	Отношение значащих бит к общему кол-ву
200	17%	0.13
300	26%	0.19
400	35%	0.23
500	43%	0.26
600	52%	0.28
700	61%	0.30
800	69%	0.31
911	79%	0.32
1000	87%	0.33
1152	100%	0.34



Процент сканируемой радужки колеблется от 40 до 99% . Есть естественные деформации границ радужной оболочки, есть болезни глаз (глаукома, косоглазие), часто мешают длинные ресницы, меняется угол отражения (зависит от выпуклости глазного яблока). Отдельная проблема – линзы, которые носит значительное число граждан. FAR в идеальных условиях может быть оценен как 10^{-6}, реально вероятность ошибки гораздо выше.

Источник: John Daugman. Recording Persons by their Iris Pattern. University of Cambridge. 2014.

Биометрия: сравнение методов



Обозначения:

1- голос

2- рука

3- лицо

4- вены

Источник: John Daugman. Recording Persons by their Iris Pattern. University of Cambridge. 2014.

Международные стандарты. Идентификация

Стандарты МСЭ (ITU-T)	Стандарты ИСО (ISO/IEC)
ITU-T X.1252 (2010) Базовые термины и определения в области управления идентификацией	ISO/IEC 24760-1:2011 Руководство по управлению идентификацией. Часть 1. Терминология и понятия
ITU-T X.1254 (2012) Структура гарантии аутентификации объекта	ISO/IEC 29115:2013 Схема обеспечения идентификации объекта
ITU-T X.1255 (2013) Структура обнаружения информации по управлению идентификацией	ISO/IEC 24760-1:2015 Общие основы управления идентификацией. Часть 2. Эталонная архитектура и требования

Некоторые основные стандарты по биометрии:

ISO/IEC 2382-37: 2012 Information Technology – Vocabulary-Part 37: Biometrics

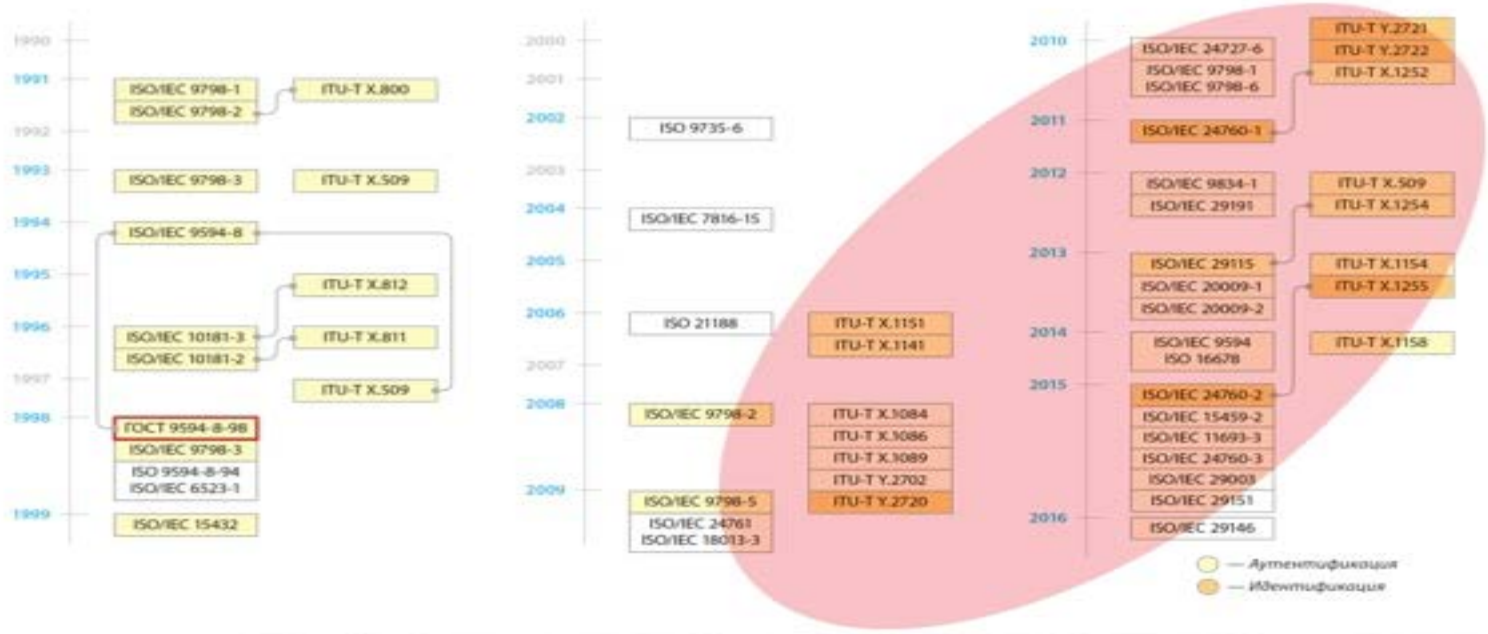
ISO/IEC 19792: 2009 Information Technology – Security Technique – Security evaluation of biometrics

ISO/IEC 19794-1: 2011 Information Technology – Biometrics data interchange

ISO/IEC 30107-1 Information Technology – Biometric presentation attack detection

США: FIPS PUB 201-2011 – Верификация идентификации.

Международные стандарты по идентификации и аутентификации



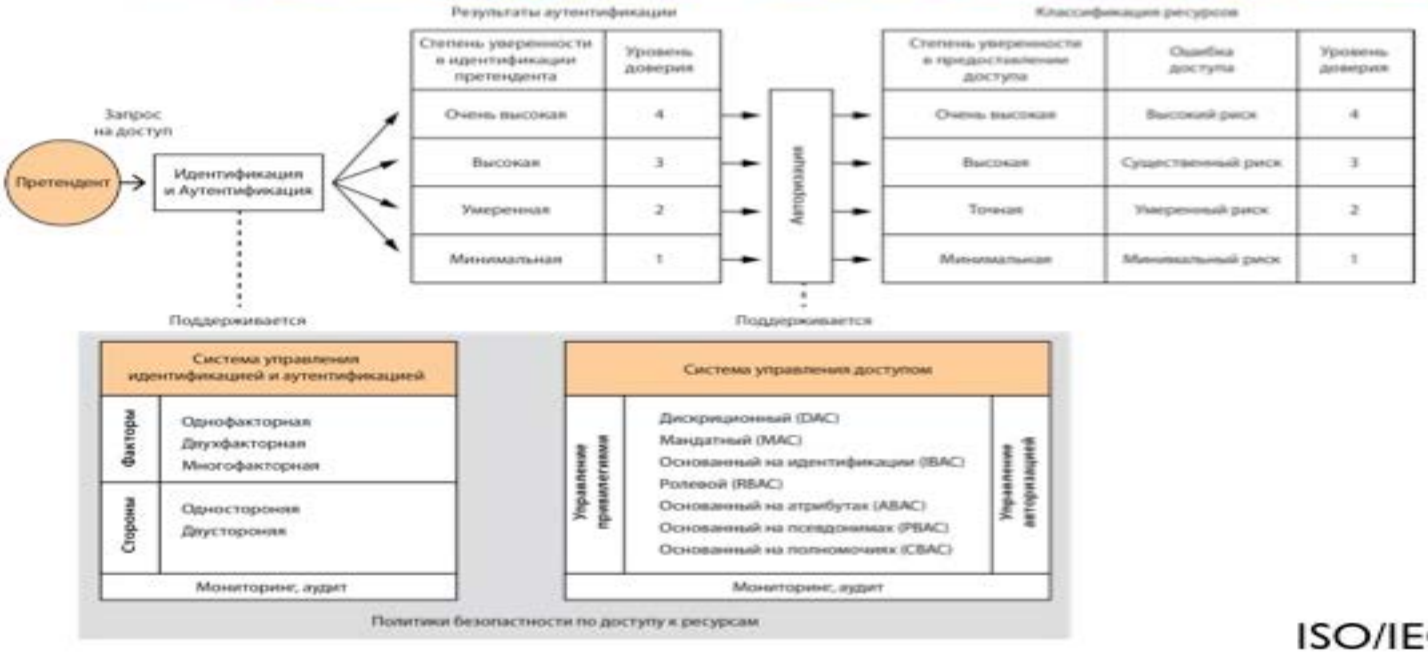
Уровни идентификации личности. ITU-T X.1154

Уровень	Описание	Задача	Средства контроля
Уровень 1 - низкий	Слабая степень уверенности в заявленной идентичности	Идентичность уникальна в рамках контекста	Собственное утверждение или заявление
Уровень 2 - средний	Определенная степень уверенности в заявленной идентичности	Идентичность уникальна в рамках контекста, и объект, владеющий идентичностью, реально существует	Проверка подлинности идентичности путем использования информации из авторитетного источника
Уровень 3 - высокий	Высокая степень уверенности в заявленной идентичности	Идентичность уникальна в рамках контекста, объект реально существует, идентичность верифицирована, идентичность используется в других контекстах	Проверка подлинности идентичности путем использования информации из авторитетного источника + верификация идентичности
Уровень 4 - очень высокий	Очень высокая степень уверенности в утверждаемой или заявленной идентичности	Идентичность уникальна в рамках контекста, объект реально существует, идентичность верифицирована, идентичность используется в других контекстах	Проверка подлинности идентичности путем использования информации из достоверного источника + верификация идентичности + личное присутствие объекта

Уровни доверия к идентификации с подтверждением

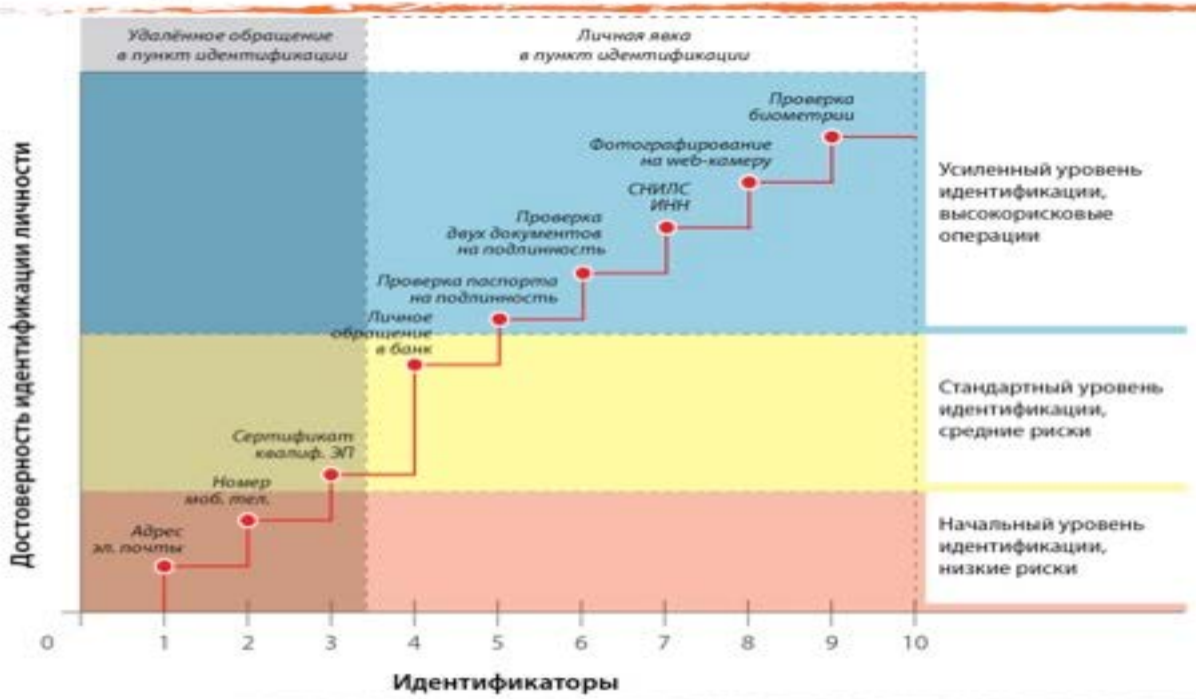
Уровень доверия	Идентификационная информация	Аутентификационная информация	Вид аутентификации
низкий	псевдоним	пароль	анонимная
средний	имя пользователя	пароль	простая
высокий	имя пользователя / заданные поля сертификата X.509, сформированного недоверенным удостоверяющим центром для доступа пользователя	одноразовый пароль (технология OTP) / закрытый ключ (ключ подписи)	усиленная
очень высокий	заданные поля сертификата X.509, сформированного доверенным удостоверяющим центром для доступа пользователя	закрытый ключ аутентификации	строгая

Взаимосвязь уровней доверия: доступ к транзакциям

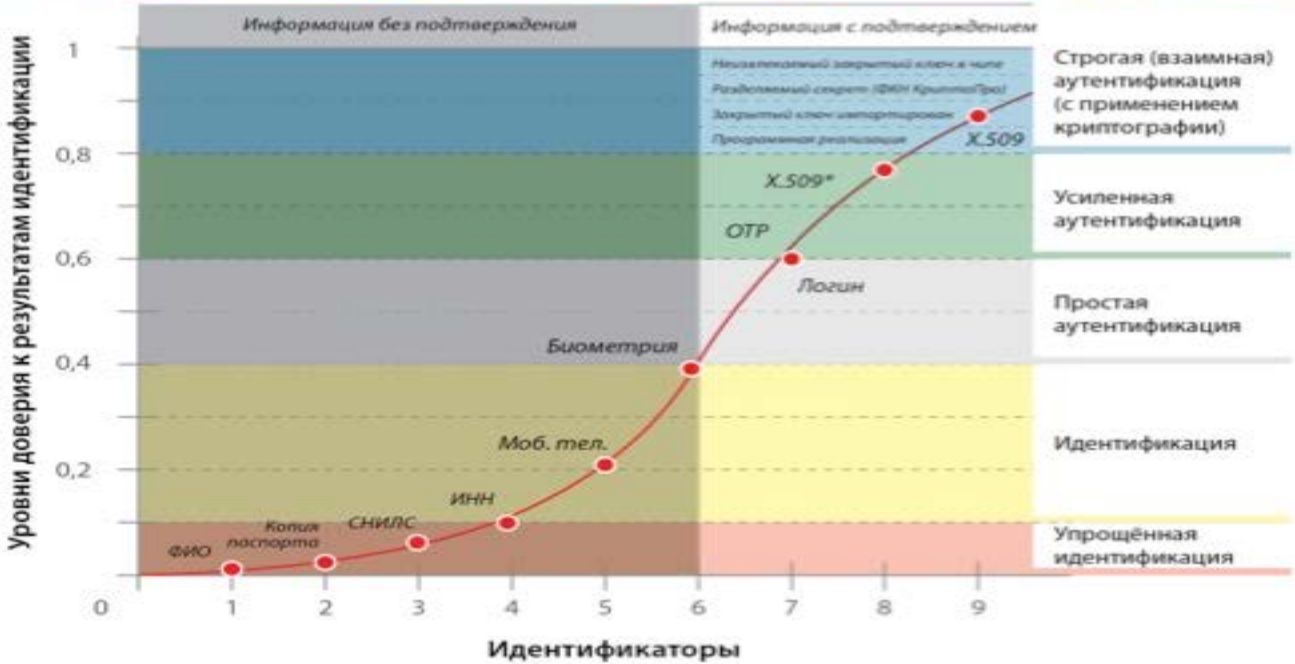


ISO/IEC 29146:2016

Достоверность первичной идентификации



Уровни доверия к идентификации



Уровни достоверности идентификации

"За" и "Против" биометрической идентификации

1.Биометрические характеристики всегда "под рукой"

2. Развитие технологий и реализаций биометрических систем позволяет их применение

3. Удобство для пользователей

1. При сравнении предъявленных биометрических характеристик с эталонными образцами решается обратная задача (идентификация объекта по представленным данным), это приводит к многократному увеличению погрешности итоговых результатов по сравнению с ошибками в исходных данных

2. Биометрия в полевых условиях (грязь, плохая освещенность, углы поворота -могут подсунуть муляж) сильно отличается от идеальных

3.Характеристики меняются во времени, нужно сопровождение эталонов

4. Любая успешная атака на базу приводит к фатальному исходу

5. Пароли можно сменить, смарт-карту переиздать, базу "био" – только новую!

6. Отсутствие внедрённых национальных проектов ID, нормативной базы, отказ части населения, дороговизна

ИТОГИ

1. К использованию биометрической идентификации следует подходить осторожно: это явно не панацея от атак злоумышленников (статистические методы с неизбежными ошибками на стадиях сбора данных, передачи и сравнения) - ISO/IEC 30107-1: 2016, стандарты ISO/IEC JTC1 SC27, ISO/IEC 19792:2009 .
2. Не определены правила и регламенты сбора, передачи и сравнения биометрических характеристик, а также ответственность за хранение базы образцов
3. В мировой практике использование биометрии опирается на национальные стратегии и реализованные проекты электронной идентификации, у нас пока

нет ни одного успешно внедрённого национального проекта ID, нормативной базы.

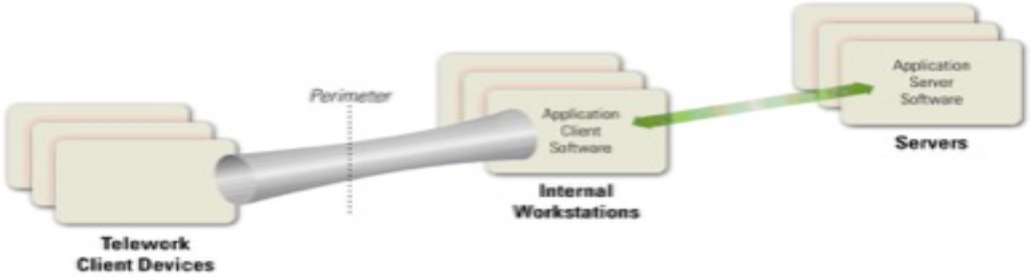
4. При внедрении неизбежен отказ части граждан и невозможность идентификации с помощью биометрии (0,32% населения и более – в зависимости от применяемой технологии) при высокой стоимости систем биометрической идентификации
5. Пока не утверждены уровни доверия к идентификации и аутентификации
6. Не определены правила передачи доверия при использовании биометрических характеристик, полученных другими организациями

Альтернативные решения: комбинированные виды усиленной аутентификации, строгая аутентификация и персональный HSM (ISO/IEC FDIS 17922-2017)

Спасибо за внимание!

a.sabanov@aladdin-rd.ru

Удалённый доступ: требования ИБ



Условия:
Отсутствие физической безопасности
Небезопасная (открытая)сеть
Инфицированные компьютеры
Возможность заражения серверов

Требования ИБ:

•Конфиденциальность – уверенность в том, что сеанс удалённого доступа и данные в хранилище (в т.ч. пользователя) недоступны третьей стороне;

•Целостность – обнаружение и блокирование любых изменений передаваемых данных;

•Доступность – уверенность в возможности предоставления удалённого доступа по требованию.

Источник: NIST SA 800-46, 2009. Guide to Enterprise Telework and Remote Access Security