Современные проблемы идентификации и аутентификации

27 сентября 2018 г.

Алексей Сабанов, к.т.н.,
МГТУ им. Н. Э. Баумана,
ЗАО "Аладдин Р.Д."

Проблемы идентификации и аутентификации

Нормативно-правовые: ни в одном документе не содержится технических требований к процессам и системам идентификации и аутентификации. На гос.уровне не имеется документов уровня Указа Президента, ФЗ. (Примеры: OMB Memorandum 04-04 2003, Homeland Security Presidental Directive 12-2004г. Identification Standart, Стратегия по аутентификации 2010г.)

Организационные: нет единого Заказчика со сбалансированными в сфере ИБ требованиями, недостаточно специалистов по идентификации и аутентификации, командуют юристы и экономисты – нет технических требований

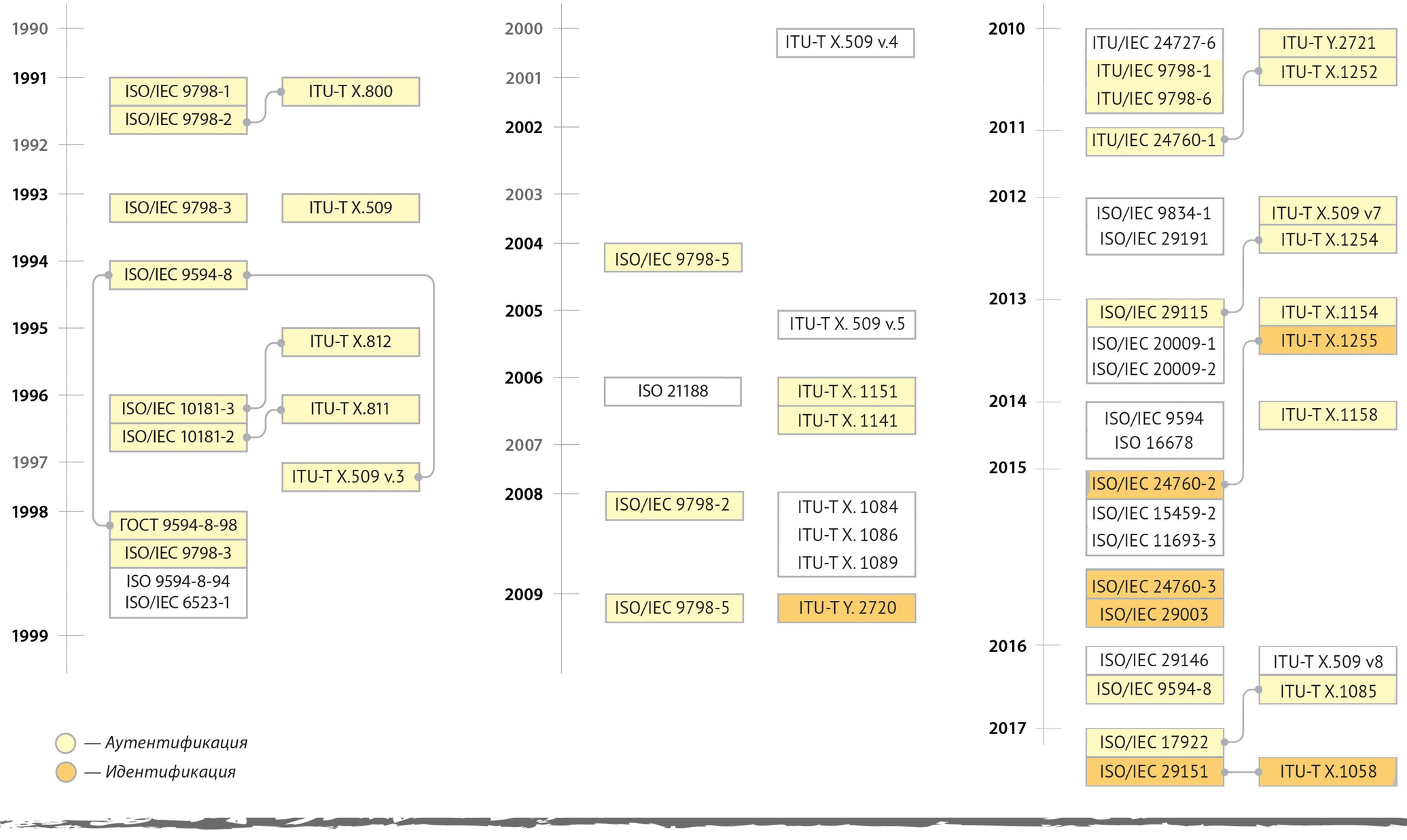
Образовательные: учебники быстро устаревают, нет лабораторных работ

Научные: нет общепринятых методов и моделей исследования, мало исследований процессов и систем идентификации и аутентификации. Отдельный научный интерес вызывают большие ИС и применение биометрии

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.

Международные стандарты по идентификации и аутентификации



Основные стандарты по теме доклада

идентификация

SO/IEC 26760-1 Identity Management Framework: General
ISO/IEC 26760-2 Identity Management Framework:
ISO/IEC 26760-3 Identity Management Framework:
ISO/IEC 29003 Identity Proofing
ISO/IEC 35 SP Identity Assurance Framework
NIST SP 800-63-3,A,B,C -2017 Digital Identity Guidelines

аутентификация

ISO/IEC 29115 Entity Authentication Assurance Framework
ISO/IEC 9798 Entity Authentication
ISO/IEC 27551 Requirements for Attribute-based uni
ISO/IEC 17922:2017& ITU-T Rec.X.1085 Telebiometric Authentication Framework using Biometric Hardware Security Module

обеспечение защиты личных данных: ISO/IEC 29100, 29101, 22307(фин.серв.) и др.

управление доступом

ISO/IEC 29146:2016 Framework for Access control
ISO/IEC 10181-3: Access Control Framework
NIST SP 800-46 Guide to Enterprise Telework and Remote Access Security: ISO/IEC 2700X

ISO/IEC 26760-2 Требования к идентификации

Идентификационные атрибуты могут храниться в реестре идентификационных атрибутов в одной или нескольких записях. Разбиение идентификационной информации на несколько записей может основываться на различиях в условиях доступа. Должно быть предусмотрено шифрование идентификационных атрибутов и их архивное хранение.

Система менеджмента идентификационных атрибутов может содержать функции:

- сервиса аутентификации, чтобы убеждаться в достоверности идентификационной информации;
- сервиса профиля, обеспечивающего стандартное представление сущностей одинакового характера;
- сервиса обнаружения, обеспечивающего возможность обнаружения других органов и установления требуемого доверия;
- сервиса обеспечения согласия в отношении приватности;
- сервиса аннулирования.

Система менеджмента идентификационных атрибутов должна специфицировать политики для операций менеджмента жизненного цикла идентификационных атрибутов:

- качества требуемой для внесения в реестр идентификационной информации;
- условий и процедуры осуществления корректировки идентификационного атрибута;
- условий и процедуры для активирования идентификационных атрибутов;
- условий и процедуры для приостановления идентификационных атрибутов;
- условий и процедуры для прекращения или архивирования идентификационных атрибутов.

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 в задаче предоставления доступа 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.

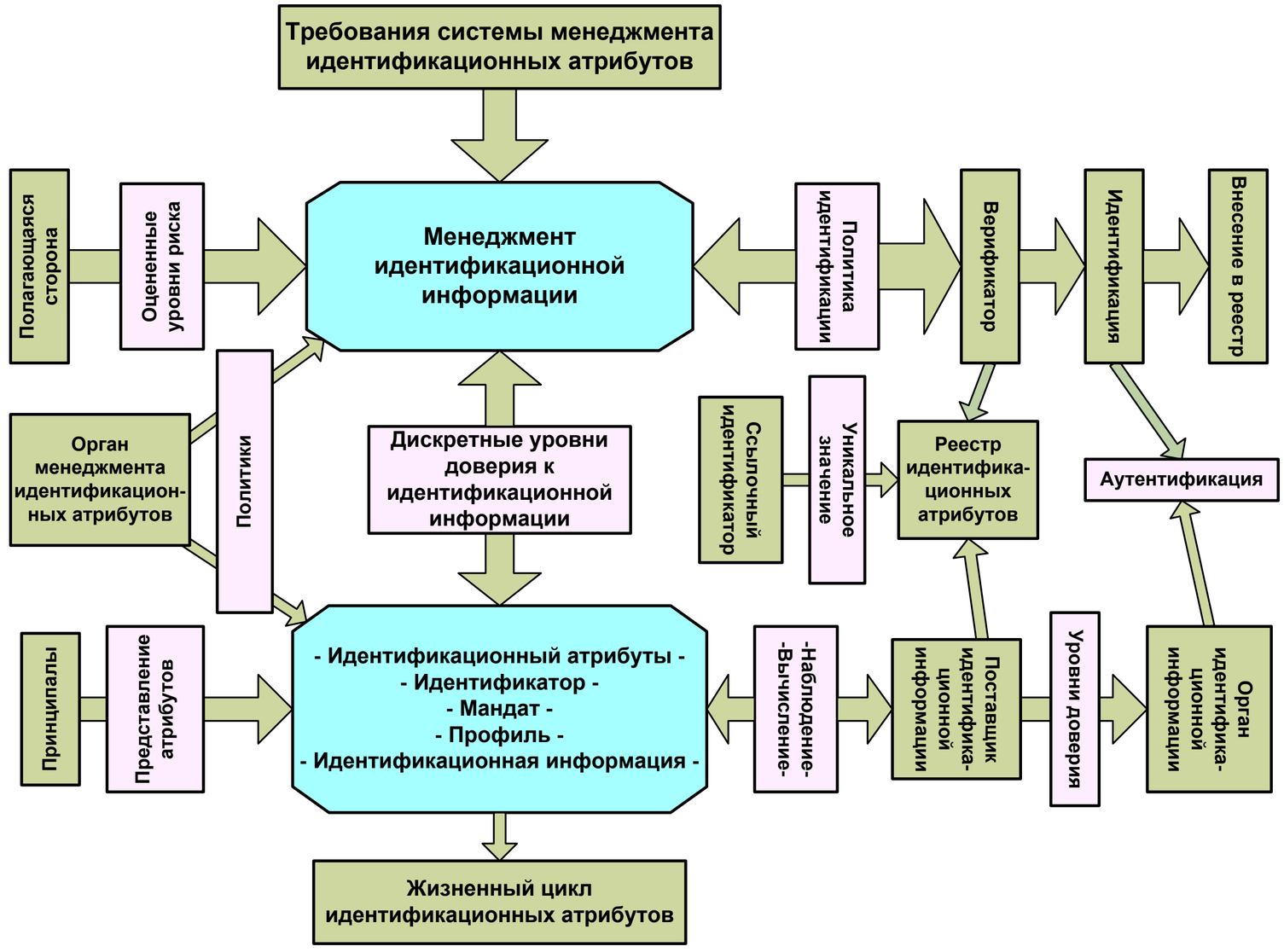
Первичная идентификация должна завершаться регистрацией (присвоением новому пользователю уникального идентификатора в данной ИС) или обоснованным отказом. Причиной отказа может являться недостаточный объем подтверждённой ИИ. Объём связанной с новым пользователем необходимой ИИ определяется политикой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

Первичная идентификация должна ответить на вопрос: тот ли это субъект, за кого себя выдает и определить возможность регистрации данного субъекта в конкретной ИС.

Участники процесса. Управление идентификацией

При запросе на доступ в конкретную ИС участники:

- Инициатор запроса на регистрацию (заявитель)
- Регистрирующая сторона
- Поставщики идентификационных атрибутов (ФНС, ПФР, ФМС,…)
- Верифицирующая сторона



Источник: ISO/IEC 26760-2

Этапы первичной идентификации

- Заявка на идентификацию субъекта
- Определение подлинности предъявленных идентификационных атрибутов и свидетельств (в том числе, официальных – паспорт, ИНН, СНИЛС)
- Сбор подтверждающей информации
- Верификация собранной идентификационной информации
- Определение того, что идентификационные атрибуты соответствуют необходимому уровню подтверждения идентификационных данных
- Привязка субъекта к идентификационной информации
- Оценка риска разглашения собранных персональных данных (152-ФЗ)
- Присвоение субъекту уникального Id в конкретной ИС и внесение в реестр Id и связанной с ним идентификационной информации
- Хранение идентификационной информации

Источники: ISO/IEC 29003, 26760-2, 3

Разница в определениях

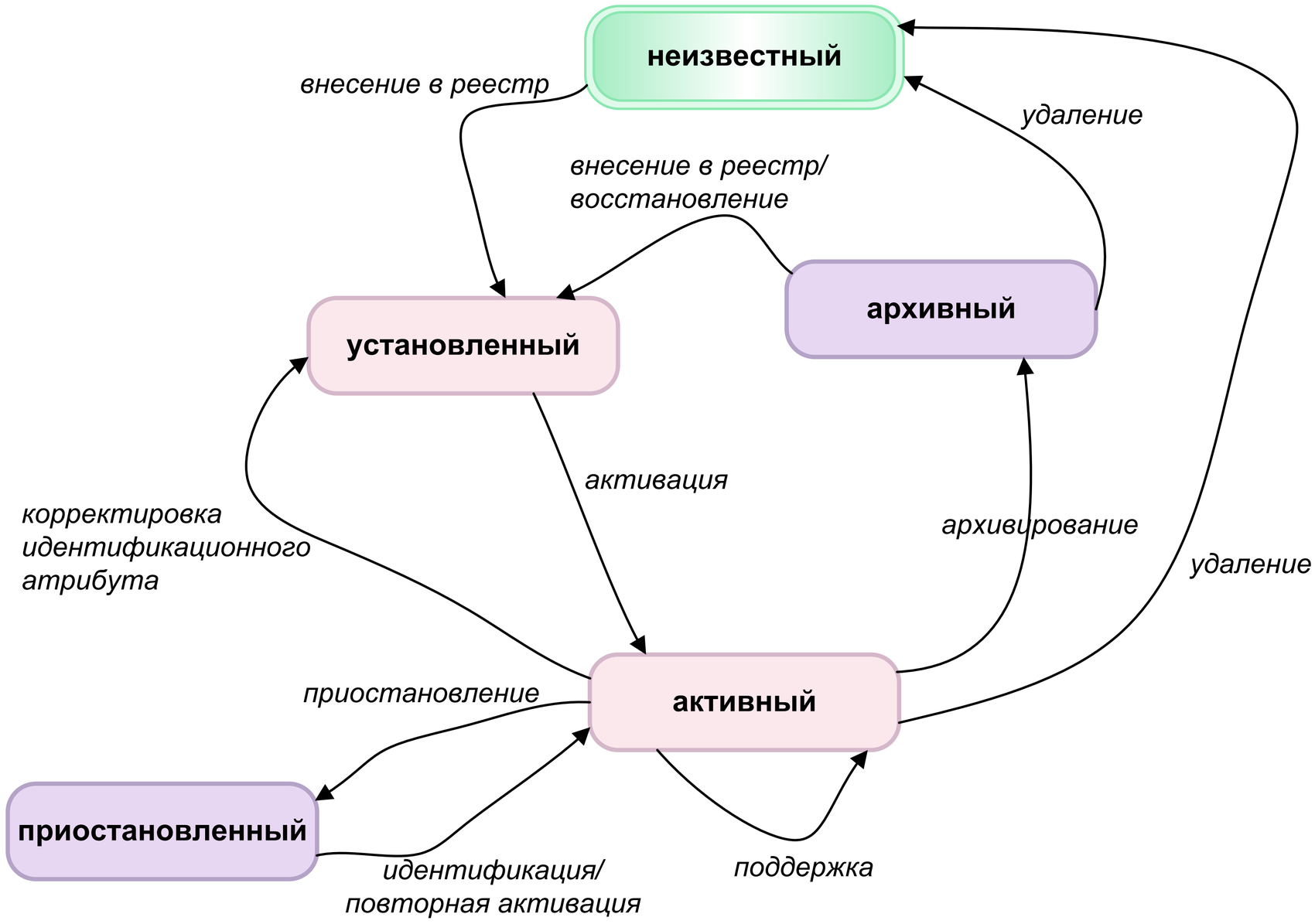
Правки в Федеральный закон 115-ФЗ, введенные Федеральным законом 482 от 31.12.2017 года, статья 4	Р 50.1.053-2005 Информационные технологии. Основные термины и определения в области технической защиты информации, пункт 3.3.9
«идентификация - совокупность мероприятий по установлению определенных настоящим Федеральным законом сведений о клиентах, их представителях, выгодоприобретателях, бенефициарных владельцах и подтверждению достоверности этих сведений с использованием оригиналов документов и (или) надлежащим образом заверенных копий и (или) государственных и иных информационных систем»	«идентификация - действия по присвоению субъектам и объектам доступа идентификаторов и (или) по сравнению предъявляемого идентификатора с перечнем присвоенных идентификаторов».

ISO/IEC 29003 Требования к подтверждению

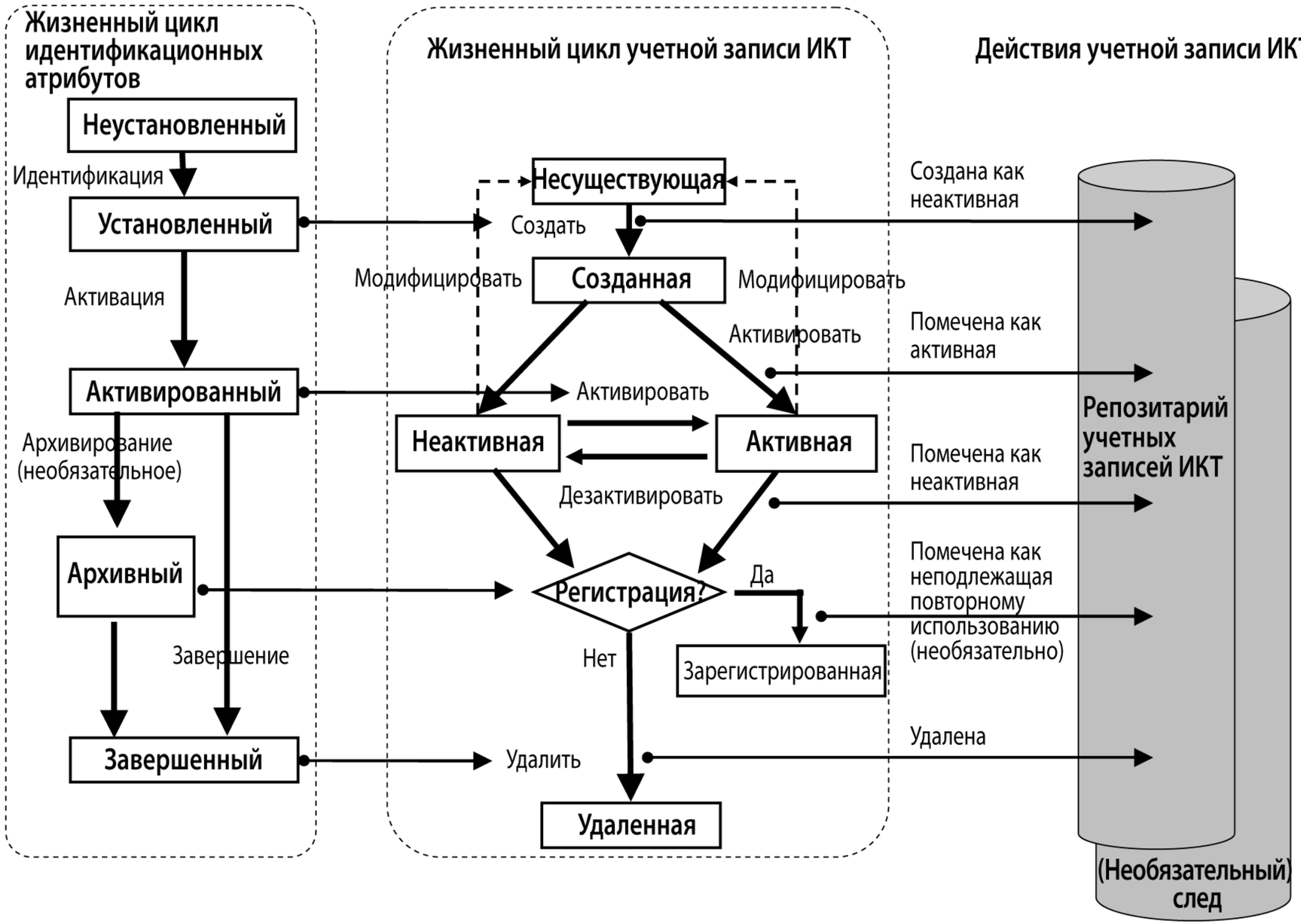
Минимальные требования к уровню подтверждения идентификационных данных относительно привязки идентификационных данных к субъекту

Цель	1-й уровень подтверждения идентификационных данных	2-й уровень подтверждения идентификационных данных	3-й уровень подтверждения идентификационных данных
Идентификационные данные привязаны к субъекту	Привязка к идентификационным данным не проверяется.	Подтверждающая сторона должна проверять привязку к идентификационным данным, используя один фактор.	Подтверждающая сторона должна проверять привязку к идентификационным данным, используя два или более факторов.

ISO/IEC 26760-2 Жизнененый цикл атрибута



ISO/IEC 26760-3 Жизненный цикл учётной записи



ISO/IEC 29003: Уровни доверия к идентификации

Уровень подтверждения идентификационных данных	Описание	Цель
1-й уровень подтверждения идентификационных данных	Низкая уверенность в заявленных или предъявленных идентификационных данных	Идентификационные данные являются уникальными в данном контексте и имеется предположение о существовании идентификационных данных и субъект предположительно привязан к идентификационным данным.
2-й уровень подтверждения идентификационных данных	Средняя уверенность в заявленных или предъявленных идентификационных данных	Идентификационные данные являются уникальными в данном контексте и умеренное установление существования идентификационных данных[a] и у субъекта есть некоторая привязка к идентификационным данным.
3-й уровень подтверждения идентификационных данных	Высокая уверенность в заявленных или предъявленных идентификационных данных	Идентификационные данные являются уникальными в данном контексте и строгое установление существования идентификационных данных[a] и у субъекта есть сильная привязка к идентификационным данным.
[a] Понятие требует совпадения значений идентифицирующего атрибута со значениями свидетельства идентичности.		

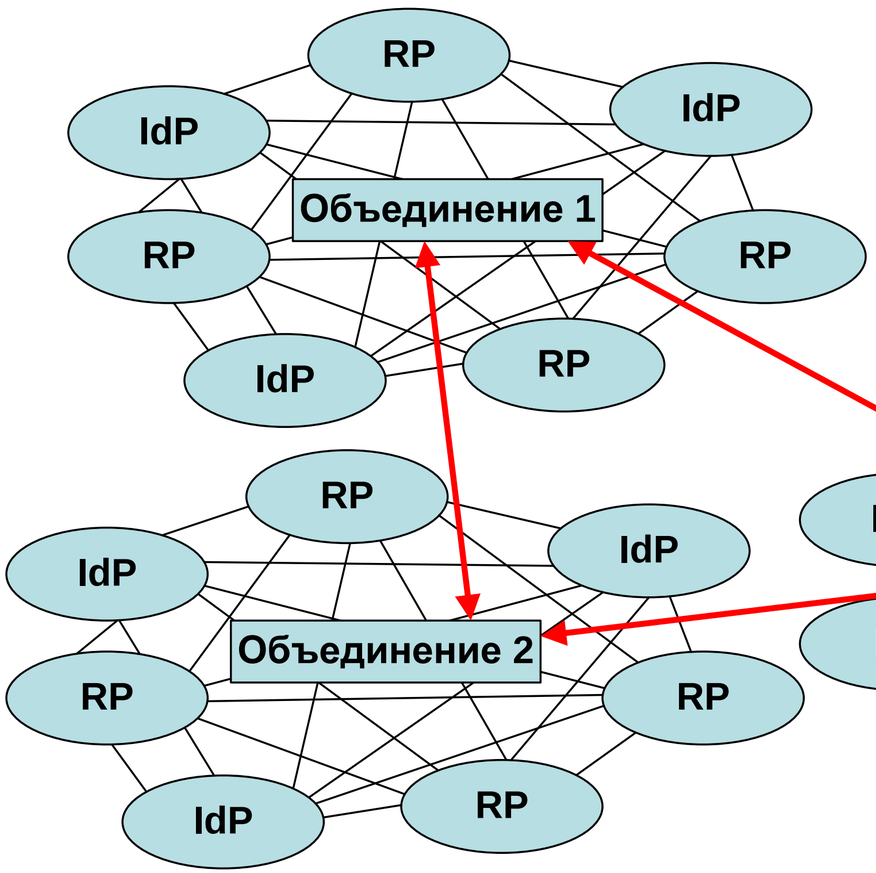
Уровни доверия к идентификации

Первичная регистрация субъекта (объекта) доступа			Допущения	Уверенность в том, что субъект (объект) доступа действительно соответствует заявленным идентификационным данным	Уровень доверия к результатам первичной идентификации	Возможность регистрации субъекта (объекта) доступа
Уникальность идентификационной информации	Подтверждение идентификационных данных					
	Существование идентификационных данных	Привязка идентификационных данных				
Заявленные идентификационные данные не соответствуют требованиям к первичной идентификации			Необходимо подтверждение идентификационных данных	Нет никакой уверенности	Доверие к идентификационным данным отсутствует	Отказ в регистрации субъекта (объекта) доступа
Заявленные идентификационные данные не соответствуют требованиям к первичной идентификации			Отсутствует необходимость подтверждения идентификационных данных	Нет никакой уверенности	Доверие к идентификационным данным отсутствует	Регистрация субъекта (объекта) доступа как «анонима»
Уникальность обеспечивается	Существование идентификационных данных не проверяется	Привязка идентификационных данных не проверяется	Необходимо подтверждение идентификационных данных	Некоторая уверенность	Низкий уровень доверия к идентификационным данным	Регистрация субъекта (объекта) доступа

Первичная регистрация субъекта (объекта) доступа			Допущения	Уверенность в том, что субъект (объект) доступа действительно соответствует заявленным идентификационным данным	Уровень доверия к идентификационным данным	Регистрация субъекта (объекта) доступа
Уникальность идентификационной информации	Подтверждение идентификационных данных					
	Существование идентификационных данных	Привязка идентификационных данных				
Уникальность обеспечивается	Существование идентификационных атрибутов и достоверность их значений в подтверждающих свидетельствах	Привязка идентификационных данных с использованием одного фактора	Необходимо подтверждение идентификационных данных	Умеренная уверенность	Средний уровень доверия к идентификационным данным	Регистрация субъекта (объекта) доступа
Уникальность обеспечивается	Существование идентификационных атрибутов и достоверность их значений в официальных свидетельствах	Привязка идентификационных данных с использованием не менее двух факторов	Необходимо подтверждение идентификационных данных	Высокая уверенность	Высокий уровень доверия к идентификационным данным	Регистрация субъекта (объекта) доступа

ISO/IEC 26760-3 Модели доверия к идентификации

Взаимодействие между **разнородными** объединениями/CoTs



- **Общие модели доверия**
- **Общие характеристики интерфейсов**
- **Функционально совместимые продукты**
- **Общие бизнес-правила/соглашения**

Примечание: красные стрелки = протоколы между объединениями;
IdP = поставщик идентификационных атрибутов; RP = полагающаяся сторона

Биометрия в идентификации и аутентификации

"Во время подтверждения идентификационных данных могут внимательно рассматриваться биометрические данные в источнике идентификационных данных с целью обнаружения попыток субъекта сделать заявки на множественные регистрации с различными идентификационными данными или сделать заявку на регистрацию с идентификационными данными другого субъекта.

Биометрическая аутентификация обычно это сравнение вида «один к одному» полученного от субъекта биометрического образца с хранящимся эталоном. Обнаружение множественных попыток регистрации требует поиска вида «один – множество» для базы данных регистрации, сравнивая полученный от субъекта биометрический образец с эталонами всех предыдущих регистраций субъекта. Поиски вида «один – множество» накладывают более строгие требования на точность используемой биометрической технологии и могут требовать использования многих биометрических образцов или модальностей.

"Биометрическое распознавание не может использоваться изолированно или вместо верификации других идентифицирующих атрибутов. Любые противоположные показания, вызванные несовпадением, необходимо исследовать специалистами в сфере биометрического сравнения, прежде чем направляться для расследования мошенничества в отношении идентификационных данных." – цитата из стандарта ИСО/МЭК 29003.

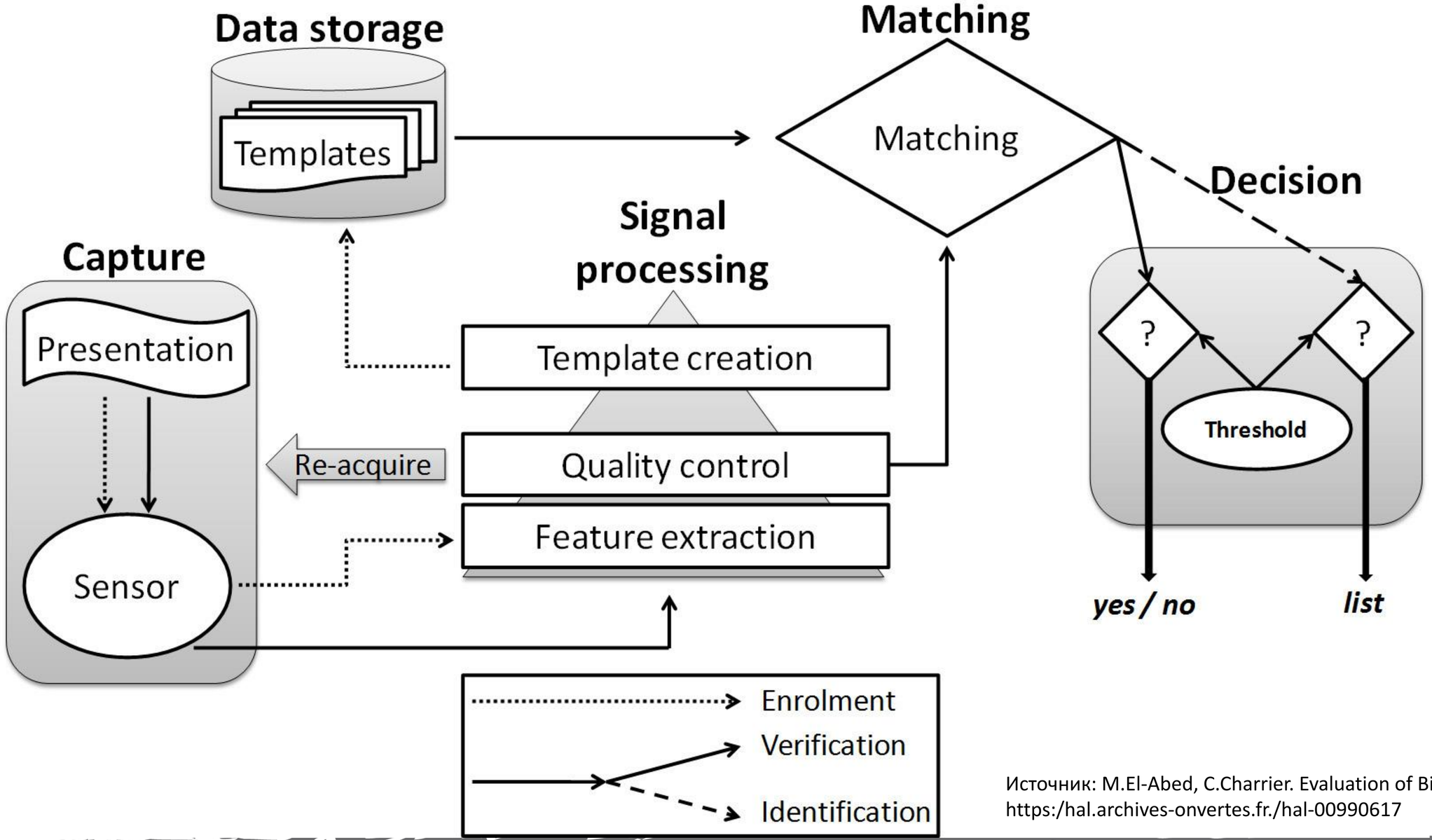
Биометрия может применяться как средство неотказуемости от регистрации (ИСО/МЭК 24760-3)

Биометрия может применяться как дополнительный фактор при аутентификации (ИСО/МЭК 29115)

Применение биометрии в идентификации

- В качестве дополнения к другим идентификационным атрибутам (данные паспорта, СНИЛС, ИНН,...)
- Подтверждение идентификационных данных: должны использоваться свидетельства, базирующиеся на действительных фактах и событиях или биометрических данных физических лиц
- Неотказуемость от регистрации
- Установление связи идентификационной информации с личностью в контролируемом периметре

Минимальный состав биометрической системы



Источник: M.El-Abed, C.Charrier. Evaluation of Biometric Systems
https:/hal.archives-onvertes.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
- В условиях удаленного приема биометрических характеристик атаки злоумышленников неизбежны
- 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

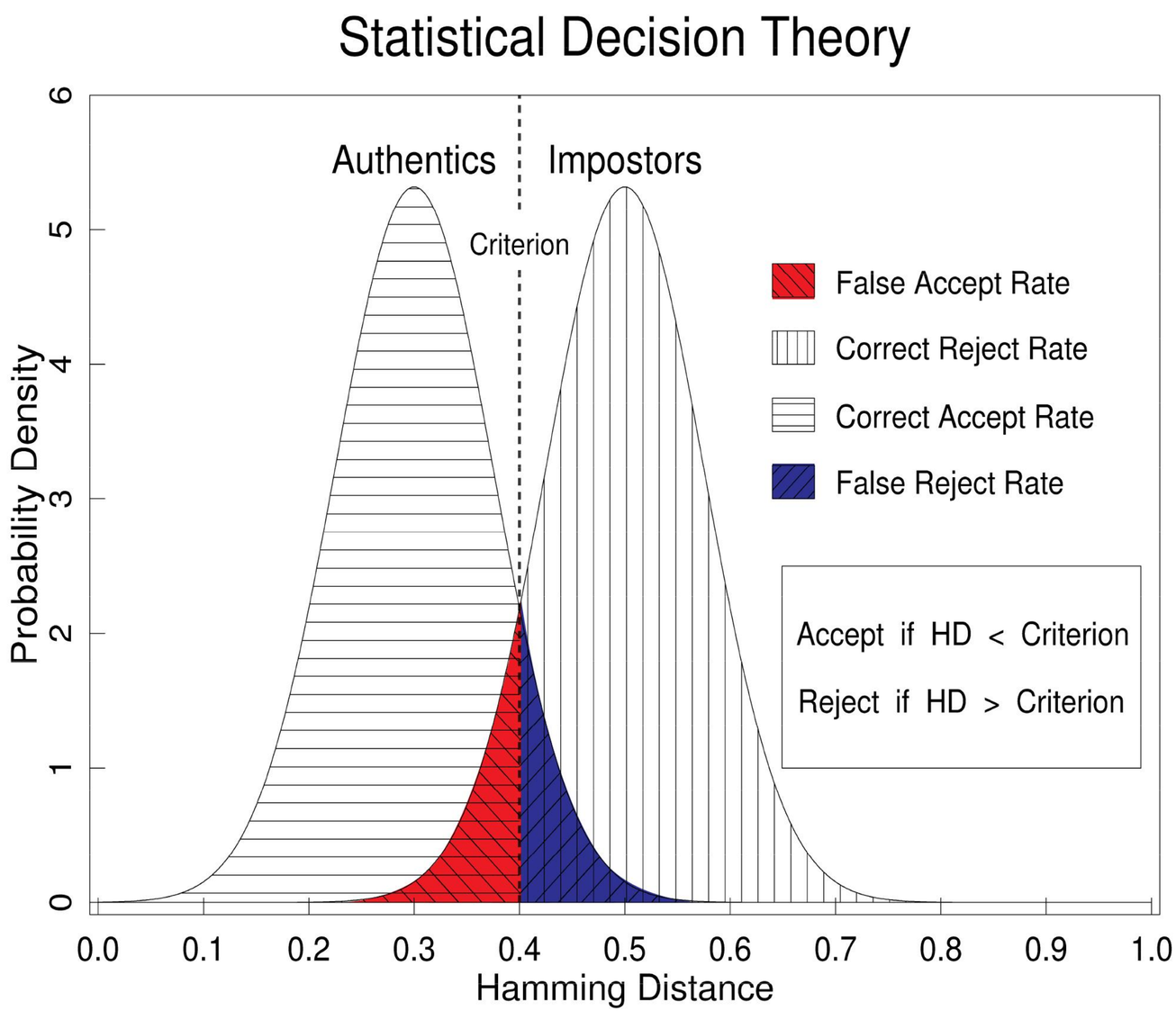
Сравнение биометрических методов

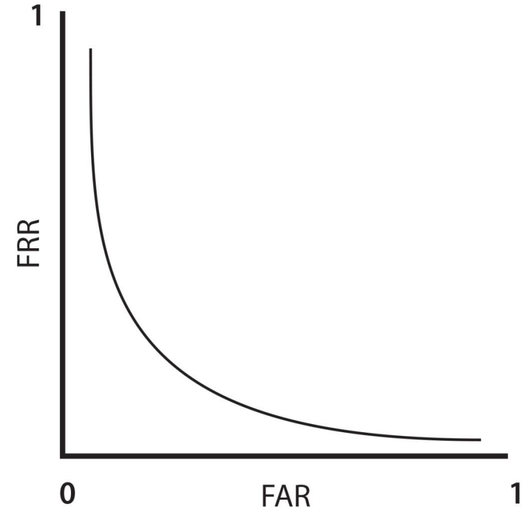
Идентификатор/критерий	Универсальность	Однозначность	Устойчивость	Простота сбора данных	Производительность	Удобство пользования	Простота обмана
ДНК	В	В	В	Н	В	Н	Н
Ухо	С	С	В	С	С	В	С
Лицо	В	Н	С	В	Н	В	В
Палец	С	В	В	С	В	С	С
Геометрия руки	С	С	С	В	С	С	С
Вены руки	С	С	С	С	С	С	Н
Радужка	В	В	В	С	В	Н	Н
Сетчатка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



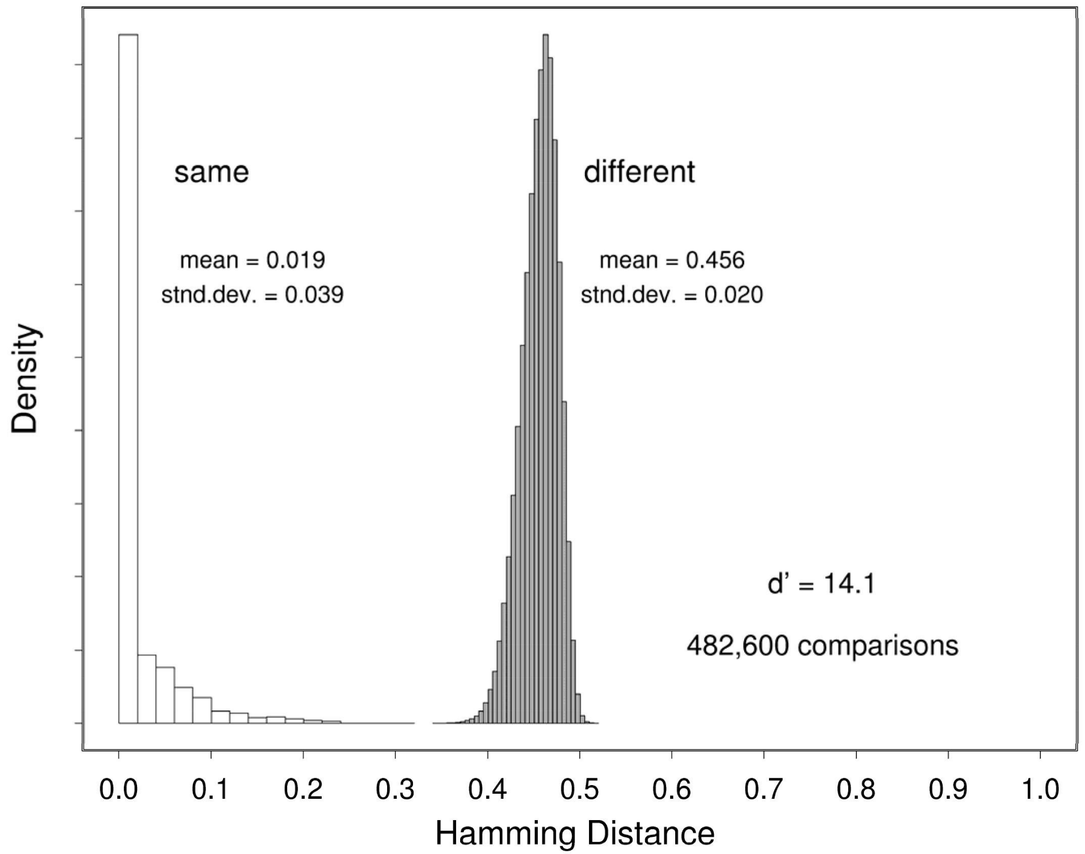


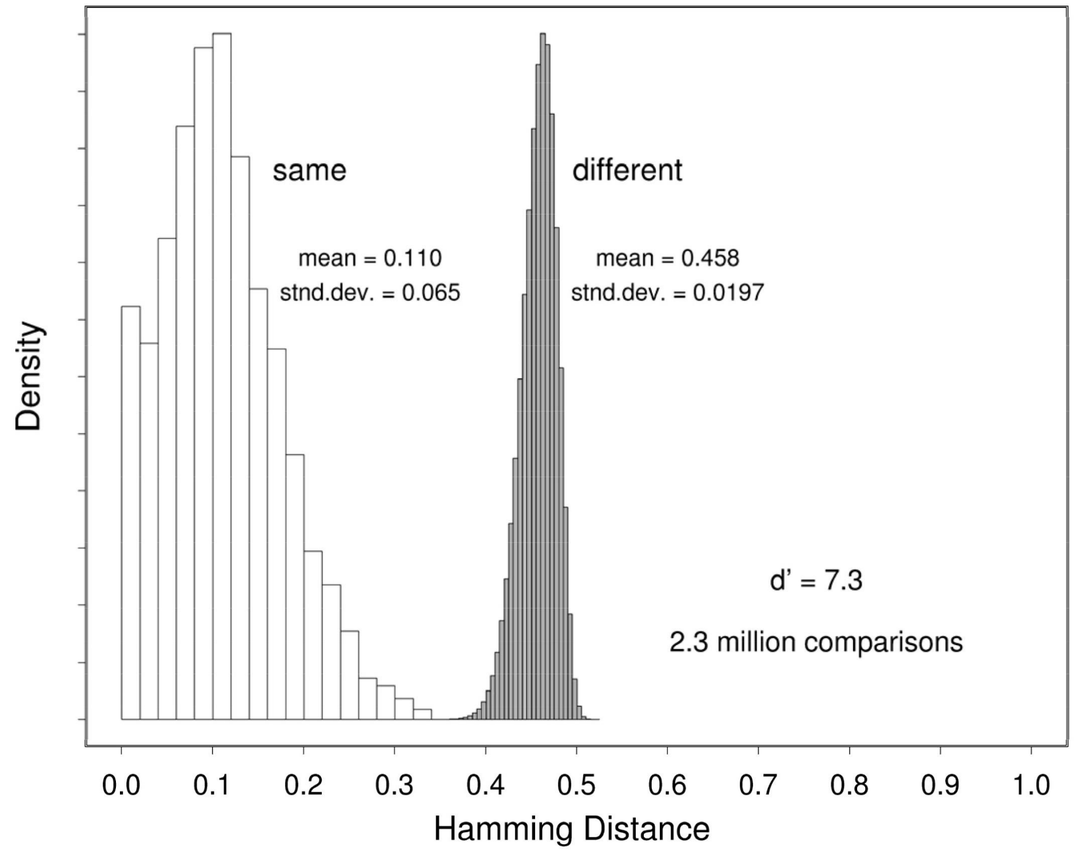
Это – теория.

На практике всё немного не так.

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

Биометрия: исследования радужки



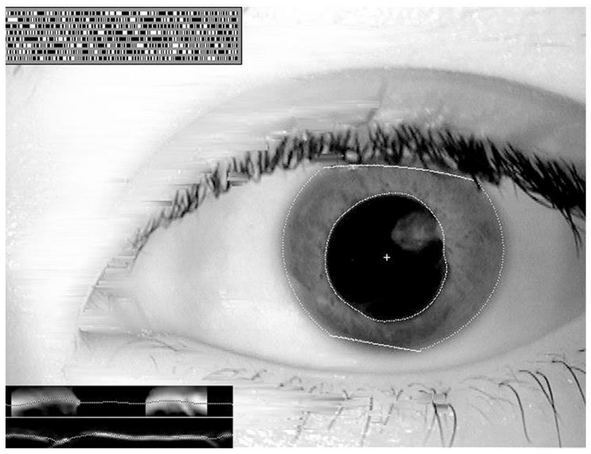


Идеальные изображения

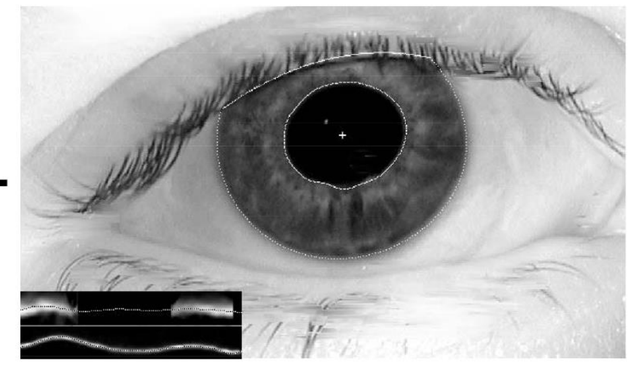
Из практики

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

Биометрия: Радужная оболочка



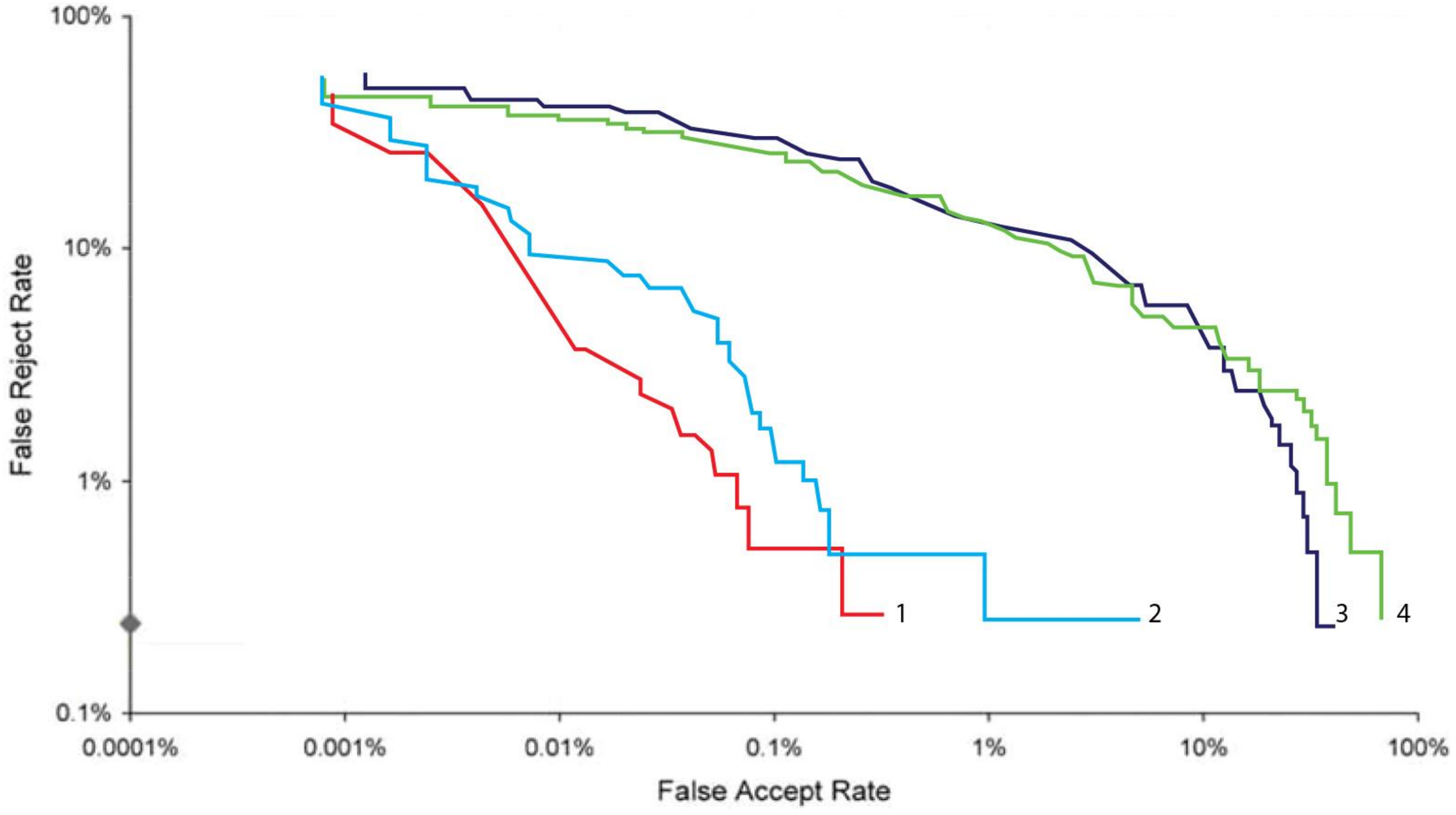
Общее число Бит	Процент видимости радужной оболочки	Отношение значащих бит к общему кол-ву
200	17%	0.13
300	26%	0.19
400	35%	0.23
500	43%	0.26
600	52%	0.28
700	61%	0.30
800	69%	0.31
911	79%	0.32
1000	87%	0.33
1152	100%	0.34



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.

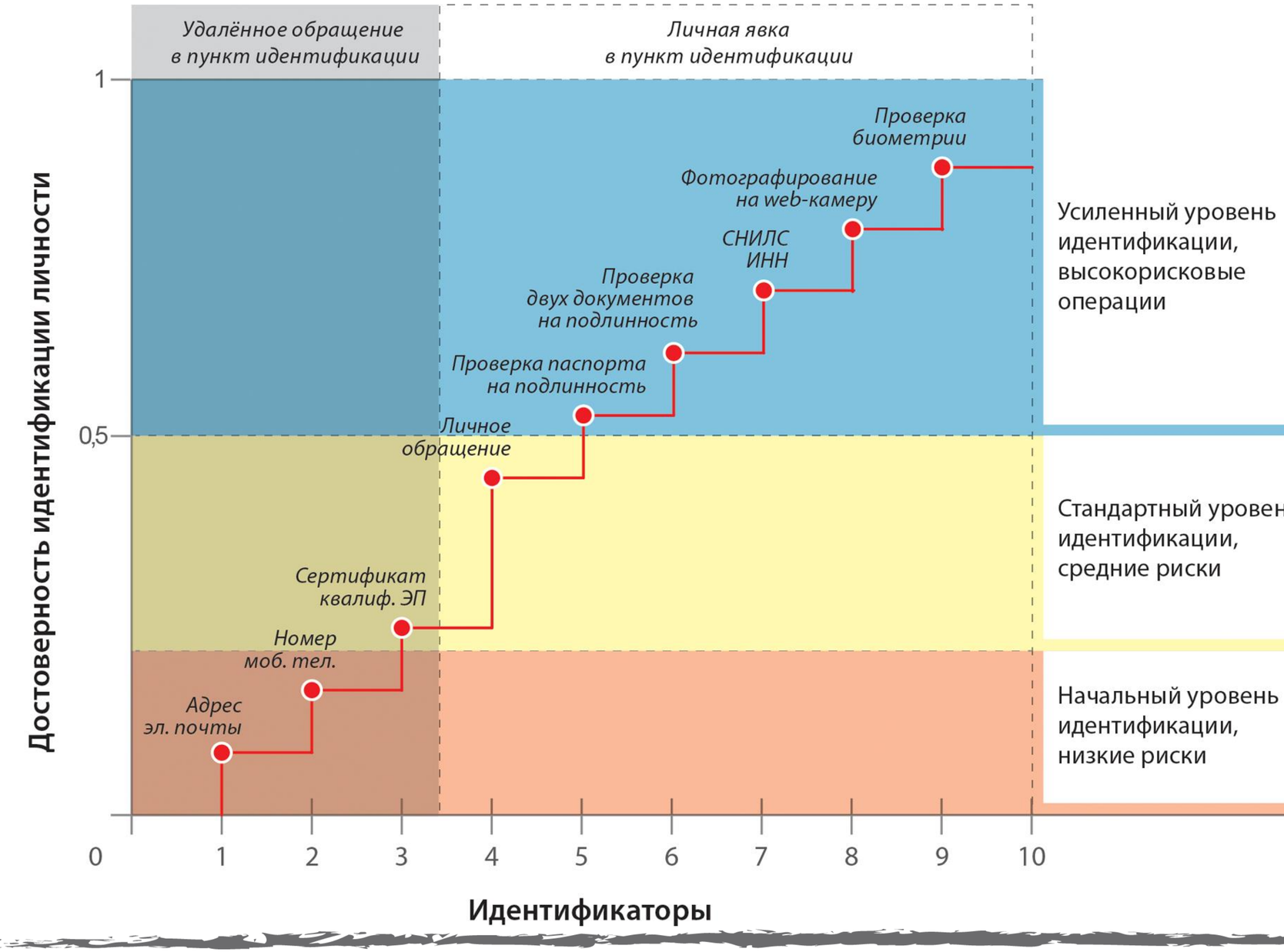
Промежуточные выводы

1. Идентификация субъектов доступа разделяется на первичную, заканчивающуюся регистрацией нового пользователя в данной ИС (однократную) и вторичную (повторяющуюся при каждом входе в ИС).
2. Для первичной идентификации введены уровни доверия, зависящие от того, проводилась ли она в личном присутствии или удалённо, и наличием подтверждённых свидетельств связи личности с идентификационными атрибутами. В западных банках при личном присутствии клиента проверяются не менее 2 документов с фотографией (фактор владения), проверяются ответы на соответствие имеющимся атрибутам (фактор знания) и опционально – биометрические характеристики.
3. Биометрическое распознавание не может использоваться изолированно или вместо верификации других идентифицирующих атрибутов.
4. При трансляции доверия идентификационных данных клиента от одной ИС к другой неизбежна потеря уровня доверия к идентификации и привязки идентификационных данных к личности.

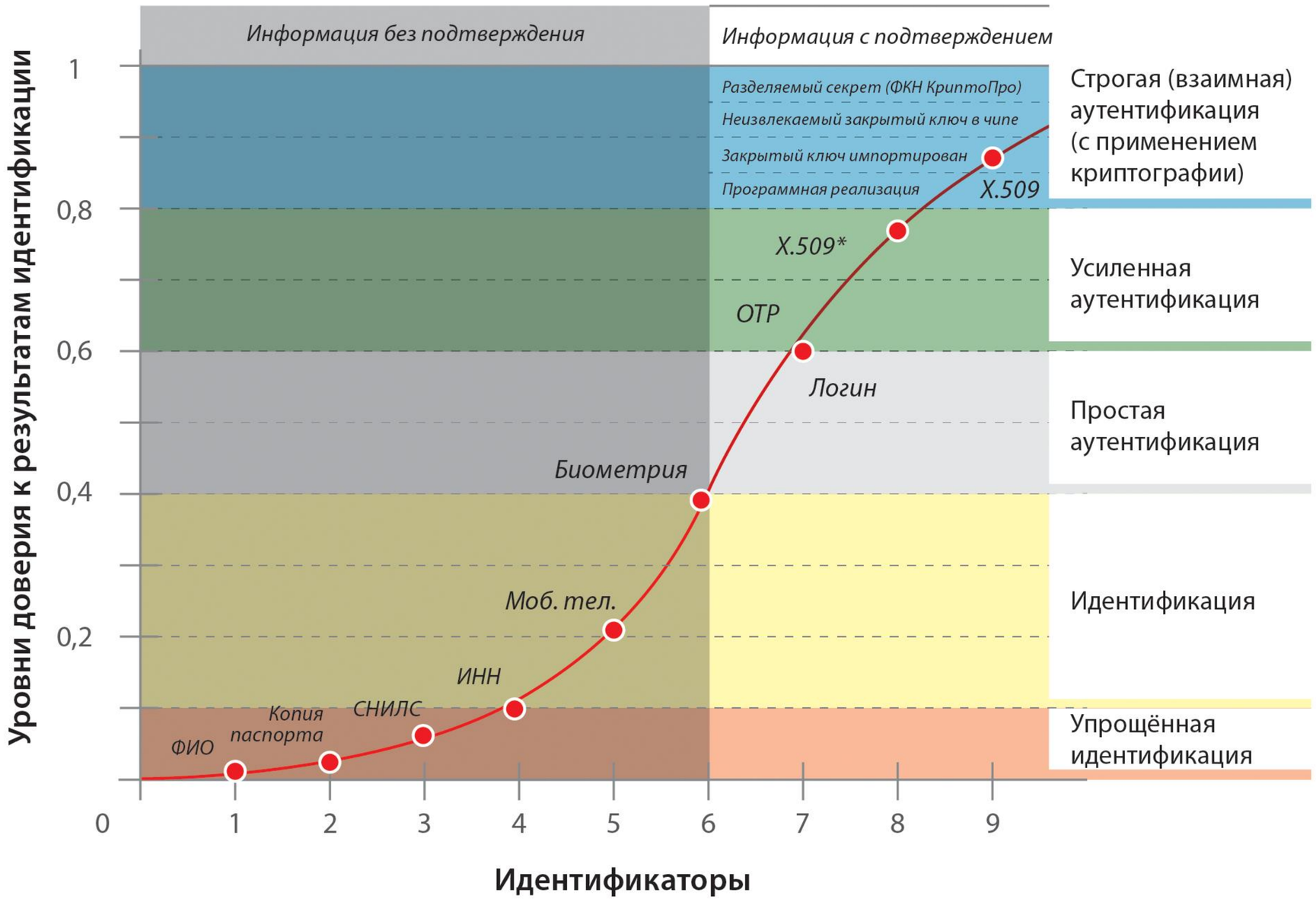
Риски удалённой идентификации (Ген.Асс.ООН)

1. Идентификация субъектов доступа – риск недостоверности собранной и подтверждённой идентификационной информации о субъектах.
2. Удостоверение пдлинности (ассоциация заявленных идентификационных данных с правильным субъектом) – риск возникновения ошибок первого и второго рода.
3. Конфиденциальность – риск раскрытия, несанкционированного или ненадлежащего использования идентификационной информации личности.
4. Защищённость данных - риск возможного получения неуполномоченной стороной доступа к личным данным физ.лиц.
5. Риск ответственности – правовая неопределённость в отношении ответственности, возникающая в связи с действием или бездействием со стороны участника системы идентификации.
6. Обеспечение исполнения – взыскание убытков в случае сбоев.
7. Риск несоблюдения нормативных положений – соблюдаются ли юридические требования по тщательной идентификации личности, получившей допуск к банковским счетам и платёжным механизмам.

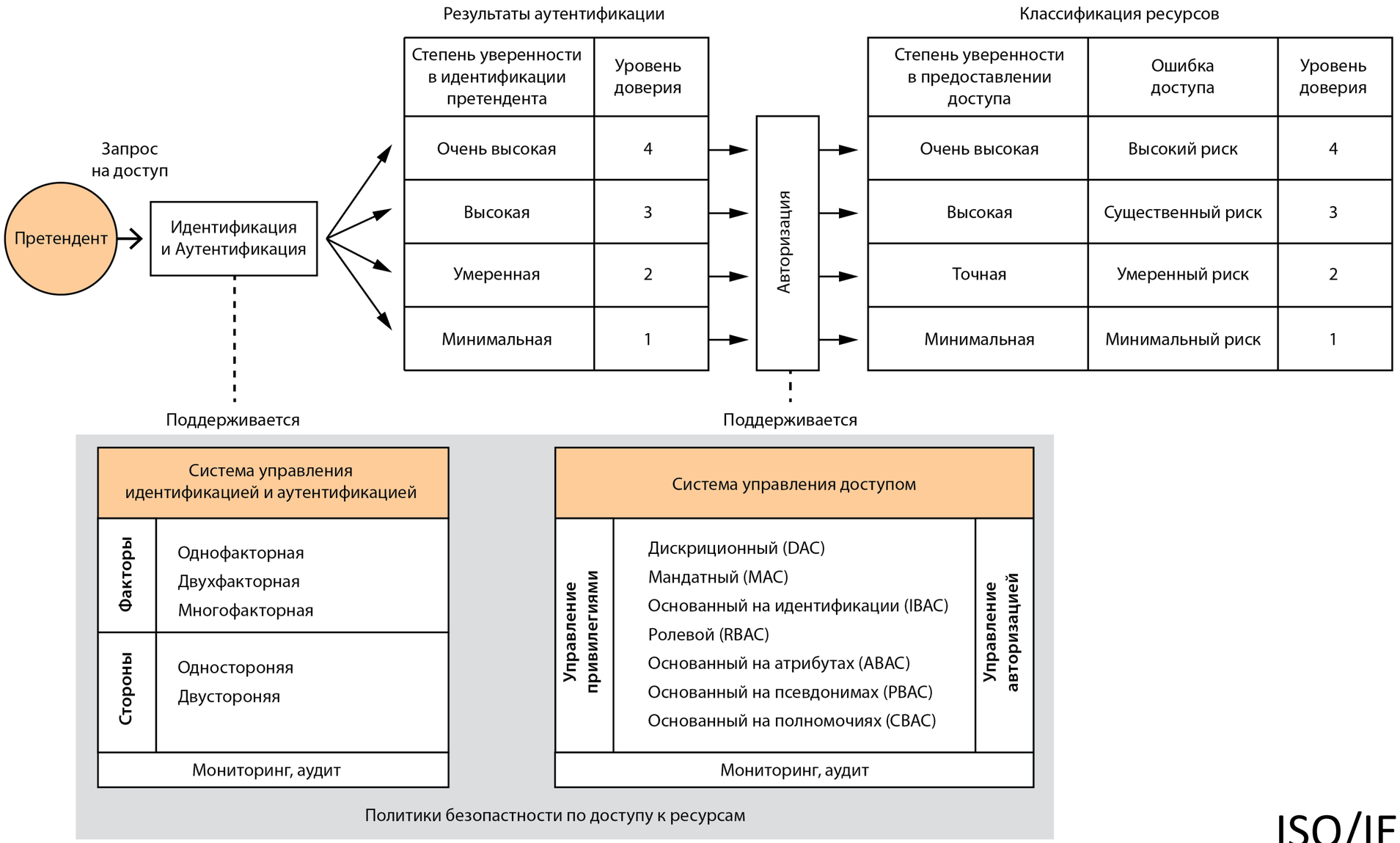
Достоверность первичной идентификации



Уровни доверия к идентификации



Взаимосвязь уровней доверия: доступ к транзакциям



ISO/IEC 29146:2016

ИТОГИ

1. К использованию биометрической идентификации следует подходить осторожно: это явно не панацея от атак злоумышленников (статистические методы с неизбежными атаками и ошибками на стадиях сбора данных, передачи и сравнения) - ISO/IEC 30107-1: 2016, стандарты ISO/IEC JTC1 SC27, ISO/IEC 19792:2009 .

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, нормативная база только начинает развиваться.

4. При внедрении неизбежен отказ части граждан и невозможность идентификации с помощью биометрии при высокой стоимости систем биометрической идентификации

5. Пока не утверждены уровни доверия к идентификации и аутентификации

6. Не определены правила передачи доверия к идентификации, тем более 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