Анализ международных стандартов по идентификации и аутентификации

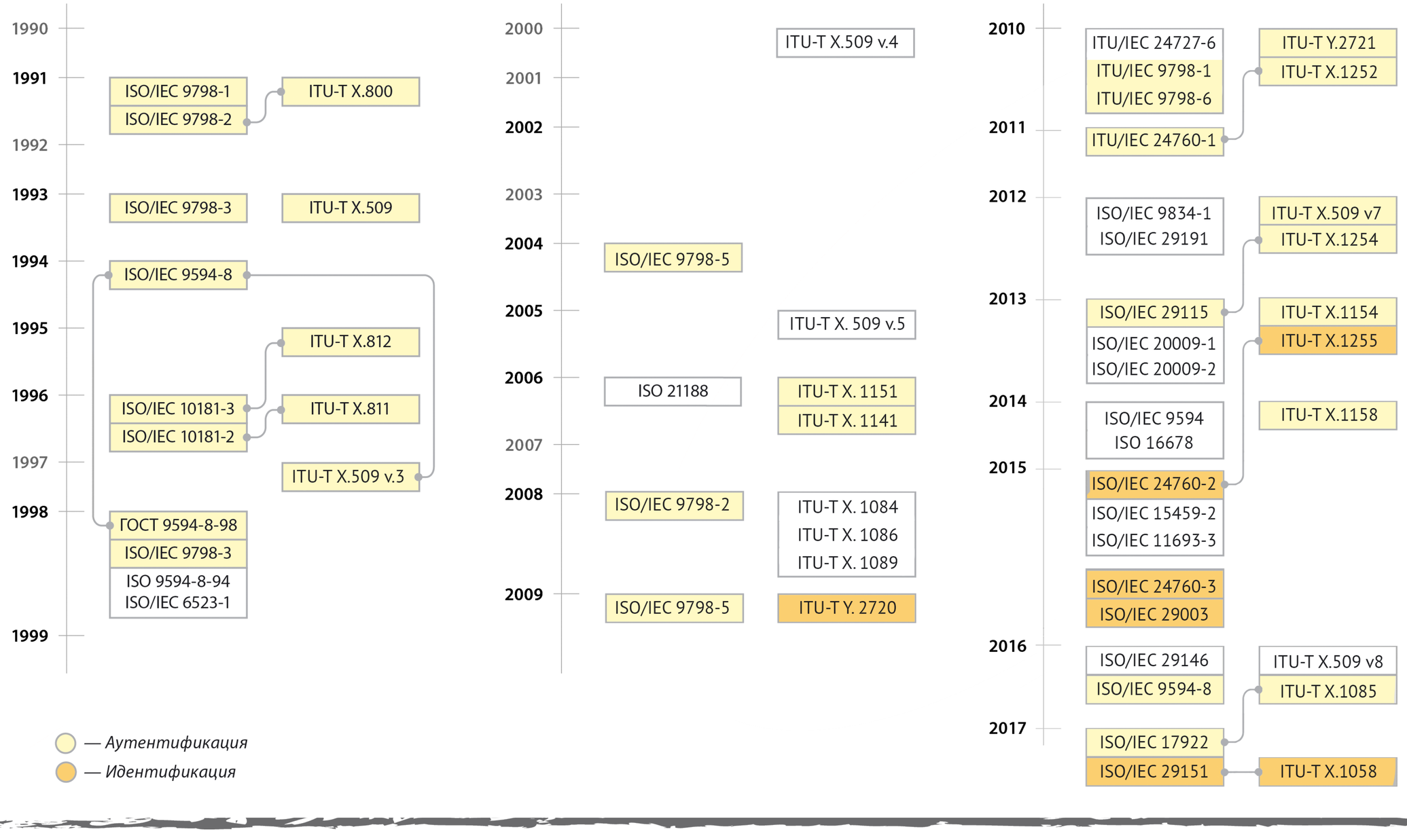
15 февраля 2018 г.

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

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

ISO/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

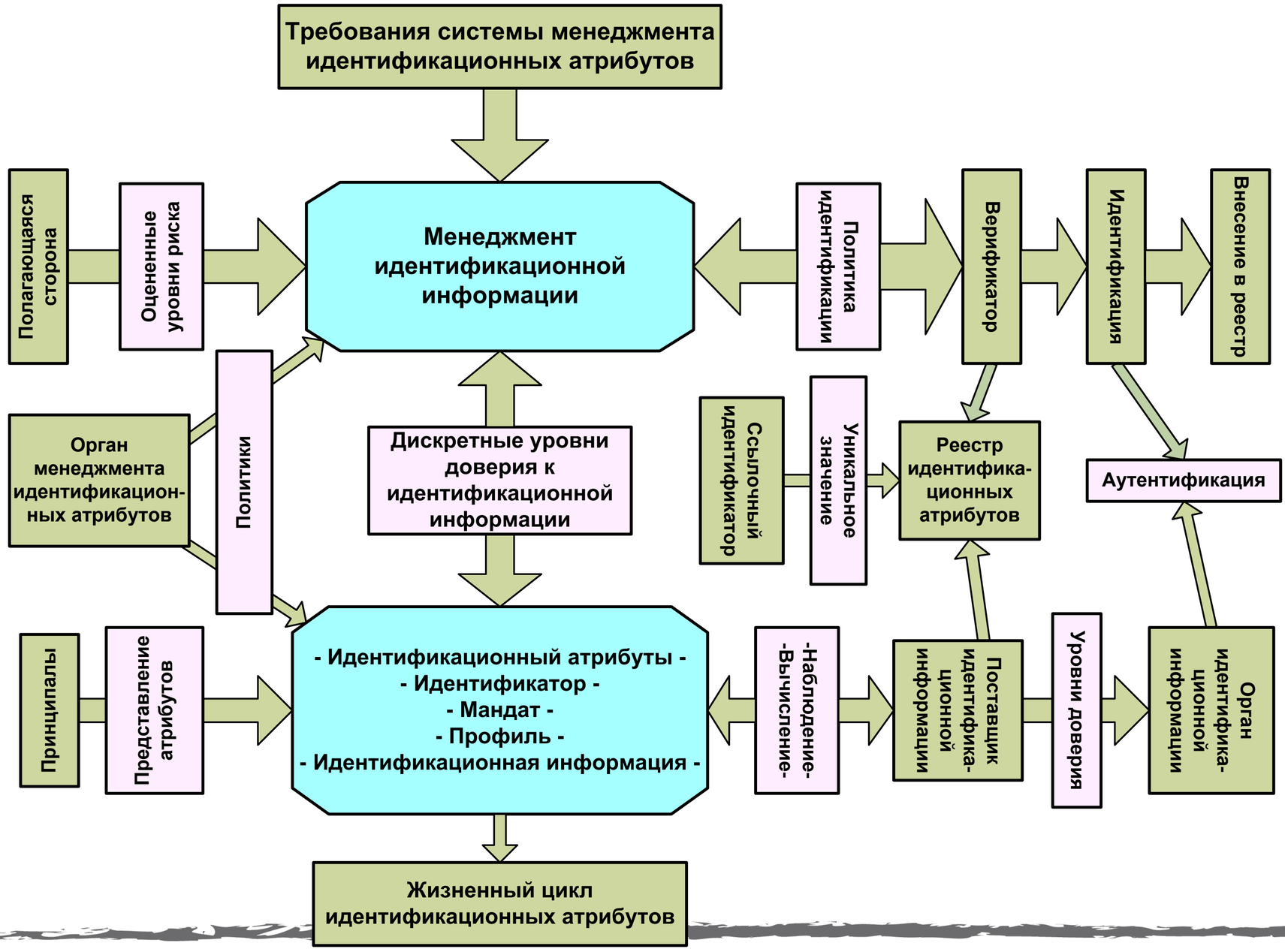
обеспечение защиты личных данных: ISO/IEC 29100, 29101, 22307(фин.серв.) и др.

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

менеджмент безопасности на основе анализа рисков: серия ISO/IEC 2700X

ISO/IEC 26760-2 Управление идентификацинными атрибутами



ISO/IEC 26760-2 Потоки идентификацинной информации

процесс	источник	получатель
Идентификация	Принципал (заявитель)	Верификатор
	Орган идентификационной информации	
	Реестр идентификационных атрибутов	
Регистрация	Верификатор	Реестр идентификационных атрибутов
	Генератор ссылочных идентификаторов	
Аутентификация	Орган идентификационной информации	Полагающаяся сторона
Генерация ссылочных идентификаторов	Принципал	Генератор ссылочных идентификаторов
Активация	Орган менеджмента идентификационных атрибутов	Реестр идентификационных атрибутов
Предоставление	Поставщик идентификационной информации	Поставщик услуг, зависящих от идентификационных атрибутов
	Орган идентификационной информации	Орган идентификационной информации
		Верификатор
Корректировка идентификационных атрибутов	Орган менеджмента идентификационных атрибутов	Реестр идентификационных атрибутов
Аудит	Реестр идентификационных атрибутов	Аудитор
	Поставщик идентификационной информации	
	Орган идентификационной информации	
	Аудитор	
Обработка идентификационной информации	Поставщик идентификационной информации	Поставщик услуг с рисками, связанными с идентификационными атрибутами
Санкционирование обработки информации	Принципал	Орган менеджмента идентификационных атрибутов

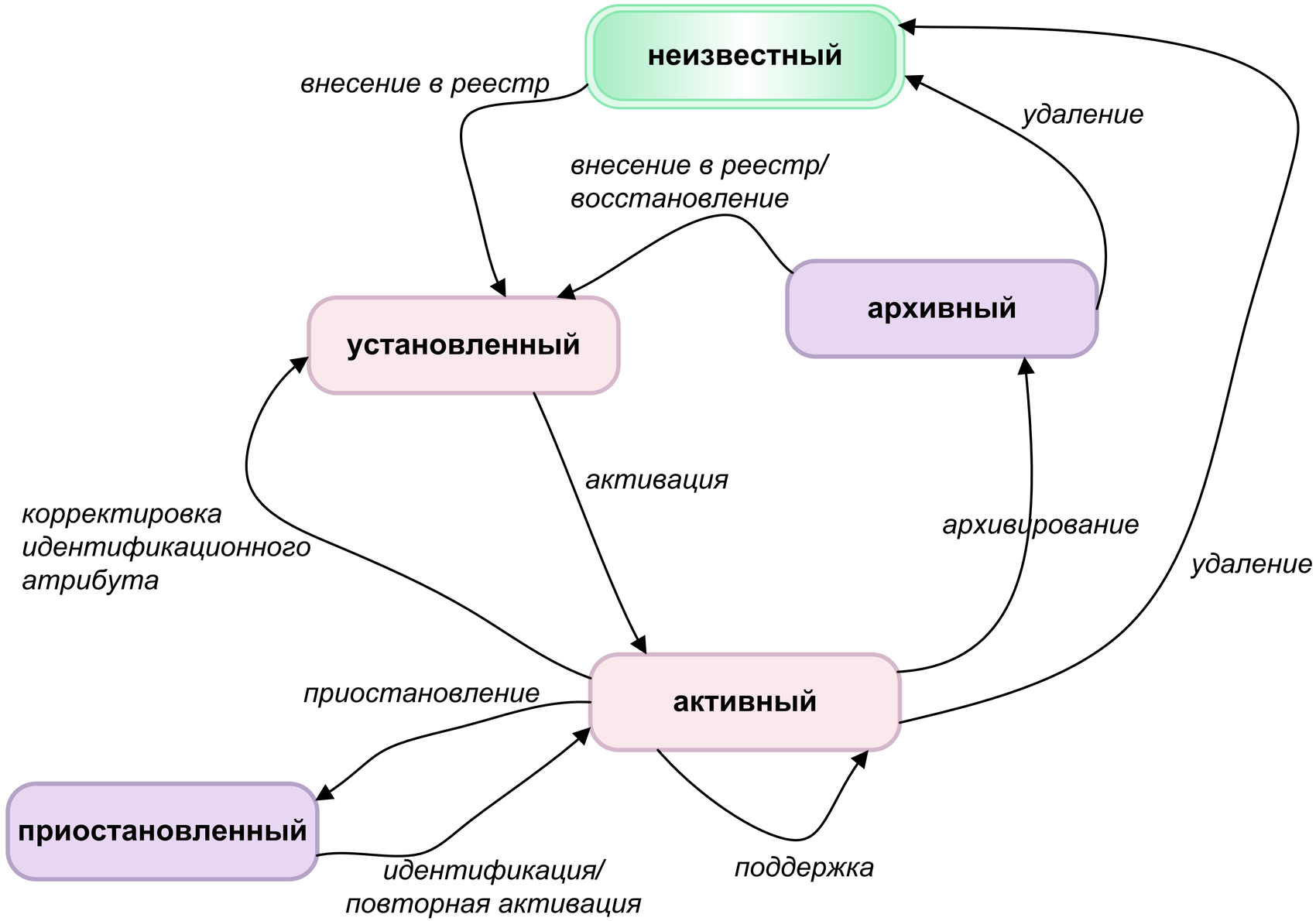
ISO/IEC 26760-2 Требования к идентификации

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.

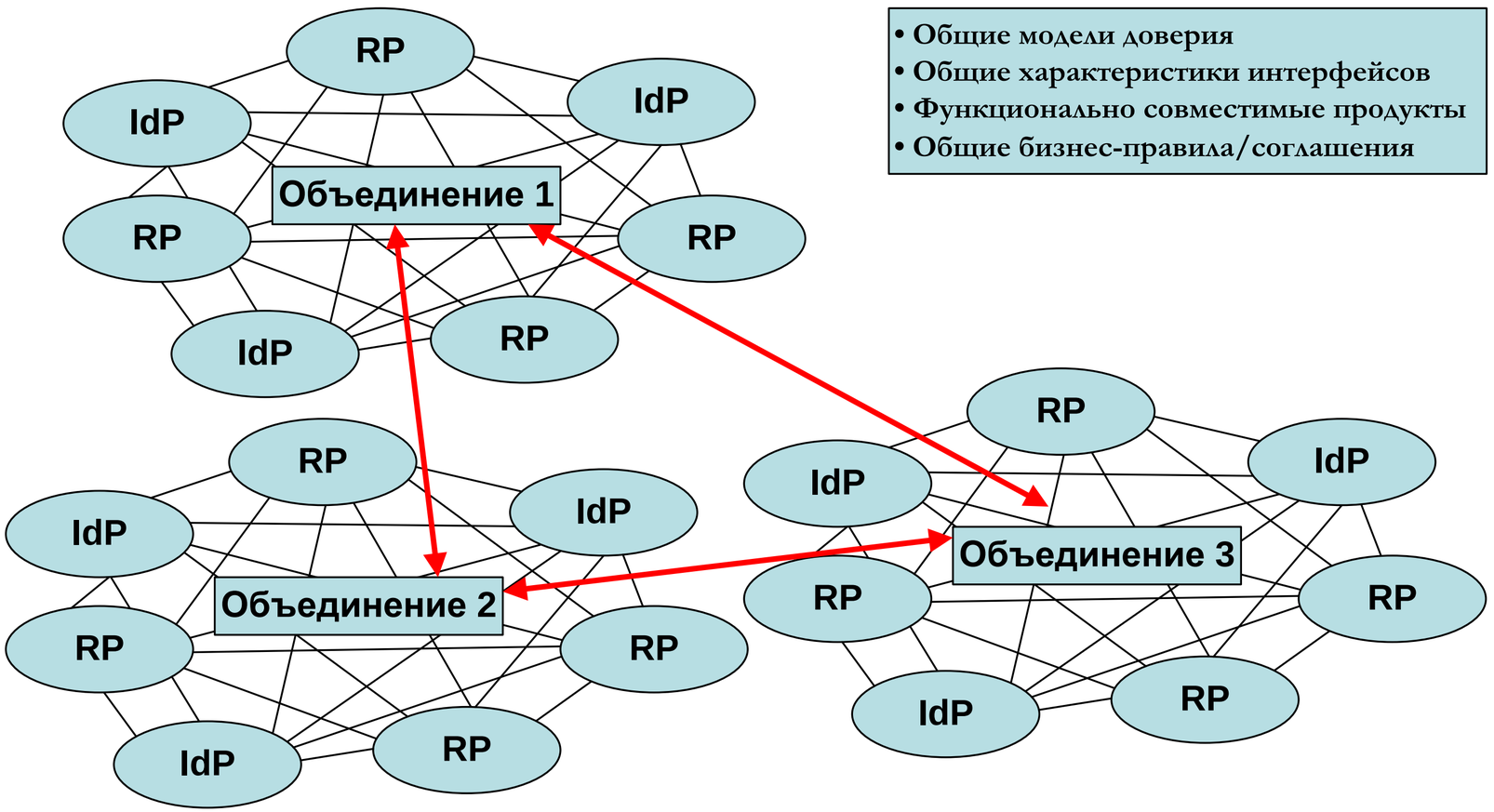
Система менеджмента идентификационных атрибутов должна специфицировать политики для операций менеджмента жизненного цикла идентификационных атрибутов:
- качества требуемой для внесения в реестр идентификационной информации;
- условий и процедуры осуществления корректировки идентификационного атрибута;
- условий и процедуры для активирования идентификационных атрибутов;
- условий и процедуры для приостановления идентификационных атрибутов;

ISO/IEC 26760-2 Жизнененый цикл атрибута



ISO/IEC 26760-3 Модели доверия к идентификации

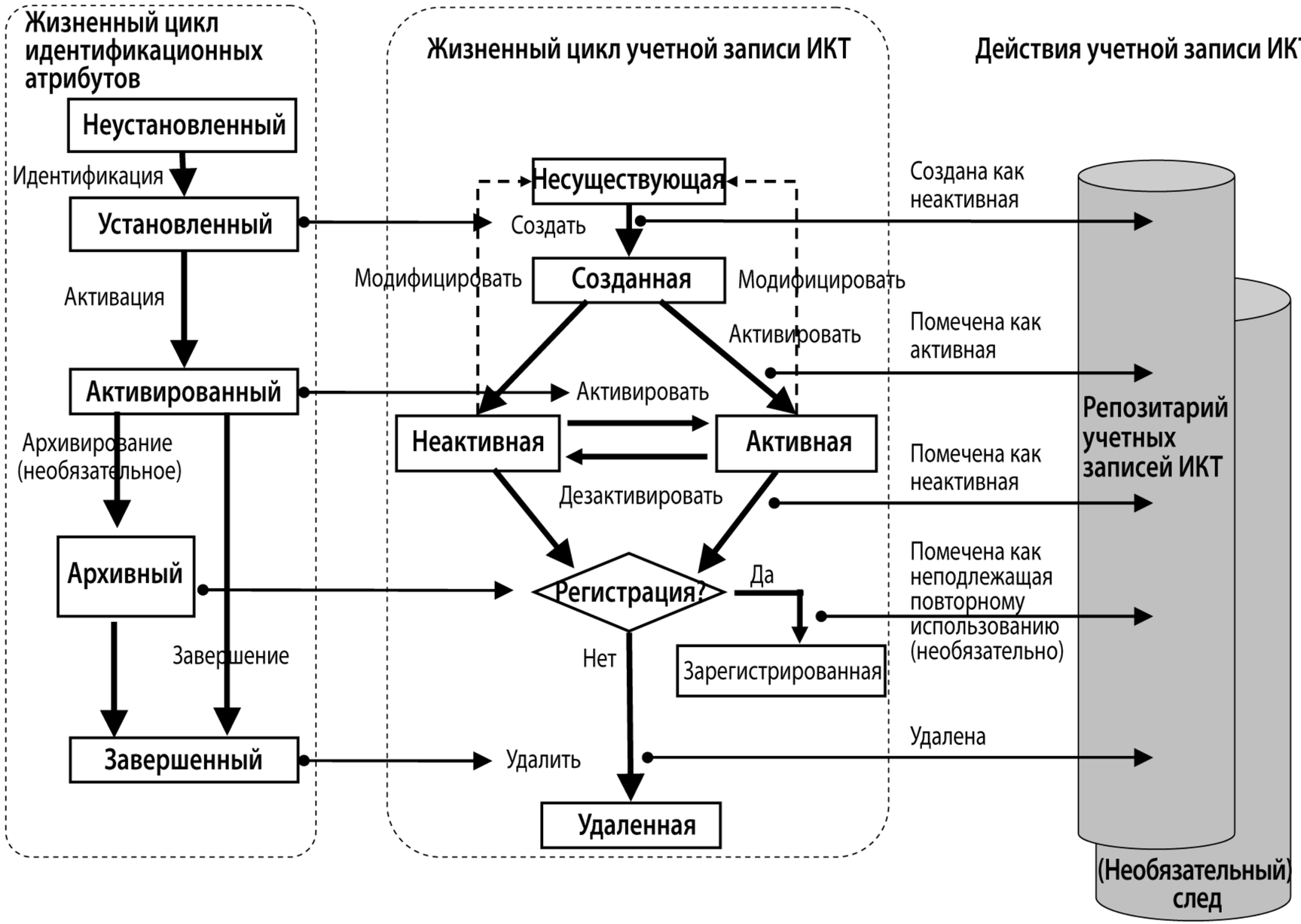
Взаимодействие между **разнородными** объединениями/CoTs



- **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

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.		

ISO/IEC 29003 Трансляция доверия к идентификации

	Идентификационные данные существуют на 1-м уровне подтверждения идентификационных данных	**Идентификационные данные существуют на 2-м уровне подтверждения идентификационных данных**	**Идентификационные данные существуют на 3-м уровне подтверждения идентификационных данных**
Идентификационные данные привязаны на 1-м уровне подтверждения идентификационных данных	1-й уровень подтверждения идентификационных данных	1-й уровень подтверждения идентификационных данных	1-й уровень подтверждения идентификационных данных
Идентификационные данные привязаны на 2-м уровне подтверждения идентификационных данных	1-й уровень подтверждения идентификационных данных	2-й уровень подтверждения идентификационных данных	2-й уровень подтверждения идентификационных данных
Идентификационные данные привязаны на 3-м уровне подтверждения идентификационных данных	1-й уровень подтверждения идентификационных данных	2-й уровень подтверждения идентификационных данных	3-й уровень подтверждения идентификационных данных

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.

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 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 подтверждённой 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.

Применение биометрии

"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 29003, приложение В.

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 трасляции доверия идентификационных данных клиента от одной ИС к другой неизбежна потеря уровня доверия 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.

Оценки ошибок удалённой идентификации

1. Достоверность первичной идентификации: вероятность ошибки от **1%** до **5%**.
2. Достоверность биометрической идентификации (оценки на основе слайда **15** прошлогодней презентации): минимальная вероятность ошибки от **1%** до **10%** (значения получены на основе обработки более **1,5** млн образцов биометрии).
3. Ошибки при передаче идентификационной информации: от **0,005** до **0,1%**.
4. Ошибки, связанные с человеческим фактором для **10** символов: от **0,6%** до **6%**.
5. При исключительно биометрической удалённой идентификации с трасляцией доверия идентификационных данных клиента от одной ИС к другой неизбежна потеря уровня доверия привязки идентификационных данных к личности, суммарную вероятность ошибки можно оценить: от **2%** до **21%**.

Промежуточный вывод: предлагаемая схема биометрической удалённой идентификации клиентов банка только по биометрическим характеристикам нуждается в совершенствовании, иначе фрод может

Как делаются оценки вероятности ошибок?

Вероятности ошибок человека-оператора(технолога)

Вид ошибки Ошибки считывания информации:	**Вероятность ошибки** [1]
• одинарного алфавитно-цифрового знака	$2 \cdot 10^{-4}$
• пятибуквенного слова при хорошем различении	$3 \cdot 10^{-4}$
• проверочного списка или цифрового показания	$1 \cdot 10^{-3}$
• десятизначного числа	$6 \cdot 10^{-3}$
Неисполнение отдельного требования при наличии памятки (инструкции) на рабочем месте	$1 \cdot 10^{-3}$
То же при отсутствии памятки и содержании в инструкции - до 10 требований - более 10 требований	 $3 \cdot 10^{-3}$ $1 \cdot 10^{-2}$
Записи числовой информации (более 3 цифр)	10^{-3} на одну цифру

Известно, что ошибки операторов наиболее часто встречаются в ИС и составляют от 15% до 30% от общего числа функционирования информационных систем.

ошибок

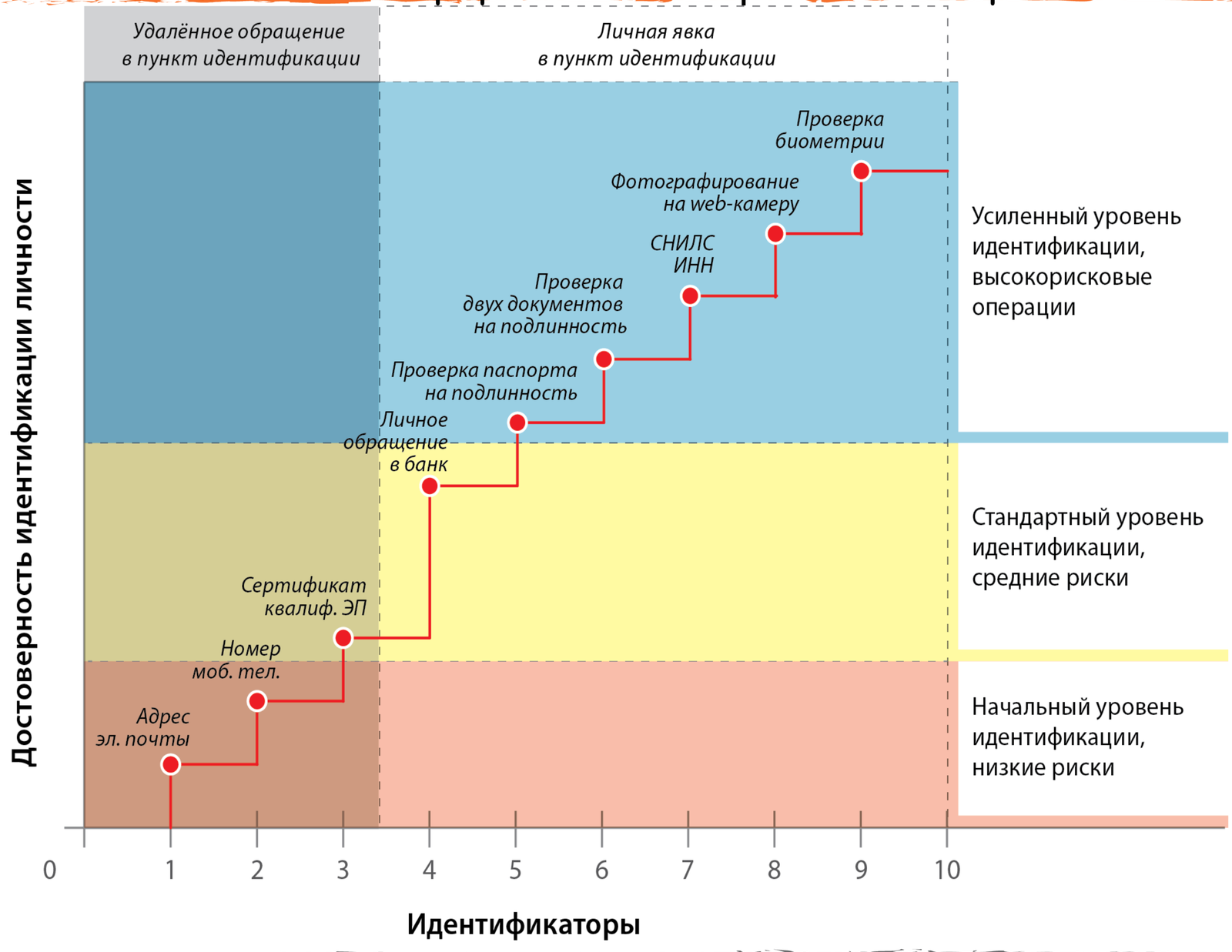
1. Шубинский И.Б. Функциональная надёжность информационных систем. Методы анализа/ И.Б.Шубинский - Ульяновск: областная типография «Печатный двор», 2012. – 296с.

Оценки ошибок при передаче

Типовое сообщение в системе идентификации и аутентификации, полученное от претендента на идентификацию представляет собой n последовательно передаваемых бит информации.
Предполагается, что канал биномиальный, т.е. вероятность k ошибок на длине сообщения n определяется как $P(k,n) = C_n^k p^k (1-p)^{n-k}$
где p – вероятность ошибки на бит; k - длина блока информационных бит, n- длина всего сообщения в битах, где N – количество байт данных сообщения; количество контрольных бит – 16 (код CRC).

При приеме сообщения должен быть реализован информационный процесс, включающий 1. проверка правильности типа пакета; 2. определение адреса отправителя; 3. определение адреса получателя; 4. проверка длины сообщения;5. проверка правильности контрольных бит (проверка контрольной суммы). Эти процессы в соответствии с уровнями иерархии упорядочиваются таким образом:1-5; 2-4; 3-3; 4-2; 5-1.
При приеме сообщения процессы выполняются в обратном порядке: вначале выполняется процесс 5, затем 4, затем 3, затем 2, затем 1.
Вероятность ошибки (трансформации) всего сообщения в предположении, что вероятность $1 - (1 - p)^{16} \approx 1$, можно оценить: $G_N = \prod_{i=1}^{4} G_i \approx [1 - \frac{1}{2^{16}} \sum_{i=r+1}^{n} C_n^i p^i (1-p)^{n-i}] \cdot \prod_{j=1}^{4} \frac{2^{16} + 1 - K_j}{2^{16}}$

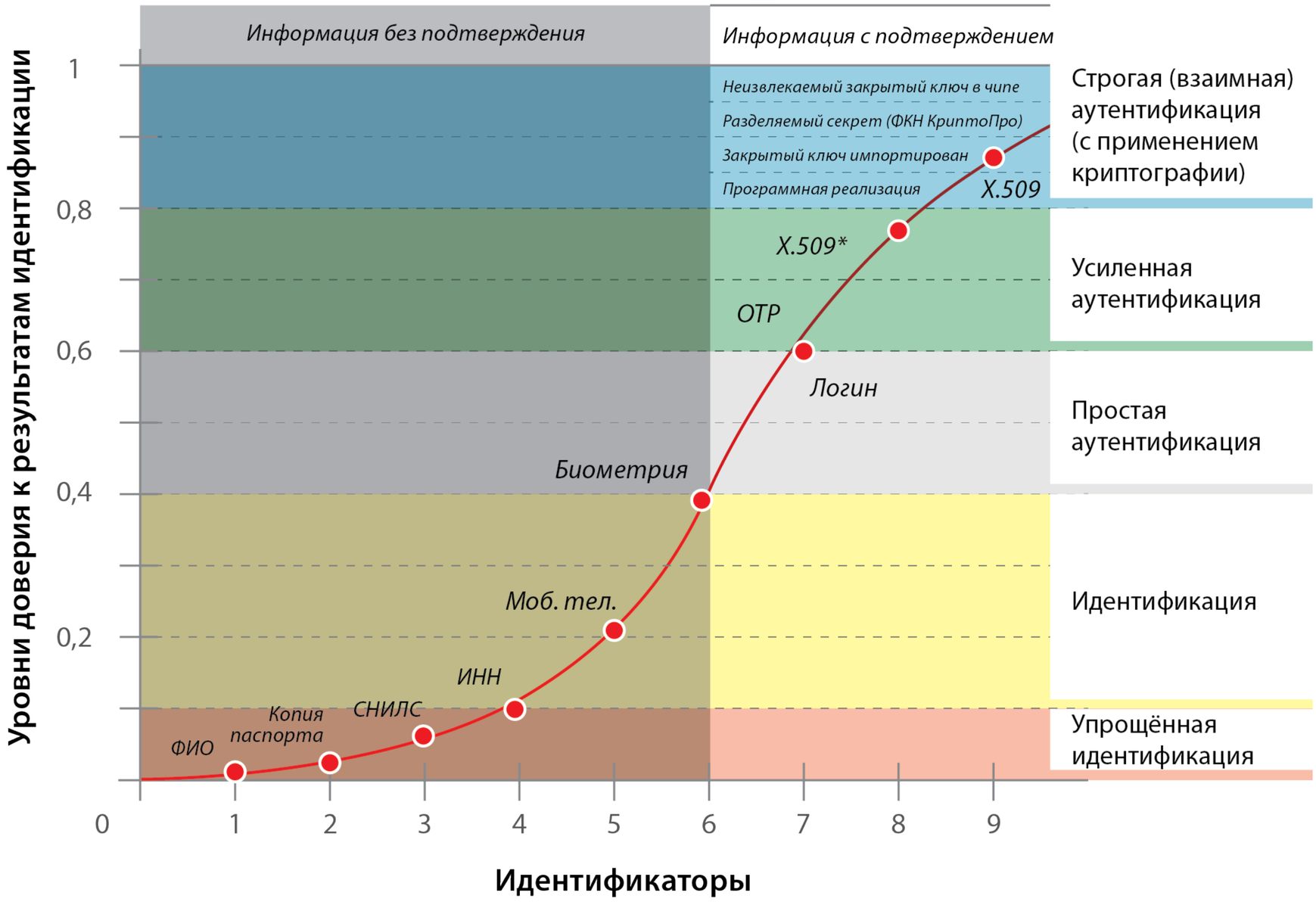
Достоверность первичной идентификации



Виды аутентификации

№	способ аутентификации	аутентификационная информация (АИ)	защита АИ	факторы	Вид аутентификации
1	запоминаемый секрет (пароль)	пароль	защита пароля от известных атак	знание	простая
2	сгенерированный заранее одноразовый пароль (пример: скрэтч-карта)	одноразовый пароль (OTP)	доверенный ДСЧ, защита канала распредлеения OTP, защита от MitM-атак	владение паролем	
3	использование второго канала (пример: телефон+SMS)	OTP	защищённая связь операций аутентификации в обоих каналах	владение телефоном	
4	устройство OTP	OTP	защита устройства	владение устройством	
5	многоразовый пароль + устройство OTP	пароль +OTP	защита устройства и многоразового пароля	владение устройством +пароль или био для доступа к устройству	усиленная
6	средство СВТ + криптографическое ПО (крипто-сервис-провайдер)	криптографический ключ	хранение ключа в TPM, TEE, хранилище ключей	владение ключом	
7	устройство (device) с установленной криптографией (СВТ либо смартфон)	криптографический ключ	неэкспортируемость криптоключа	владение СВТ + знание пароля	
8	СВТ с установленной криптографией (CSP, Kerberos) и доступом к ключу по паролю	криптографический ключ	неэкспортируемость криптоключа, доступ к нему по паролю	владение СВТ + знание пароля	строгая
9	средство СВТ + отчуждаемое устройство (SSCD) с криптографией на борту	криптографический ключ	генерация и хранение криптографического ключа в чипе Secure by Design	владение устройством + знание PIN-кода	

Уровни доверия к идентификации



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 к идентификации, тем более при использовании биометрических характеристик, полученных другими организациями

Альтернативные решения: комбинированные виды усиленной аутентификации,

Спасибо за внимание!

a.sabanov@aladdin-rd.ru