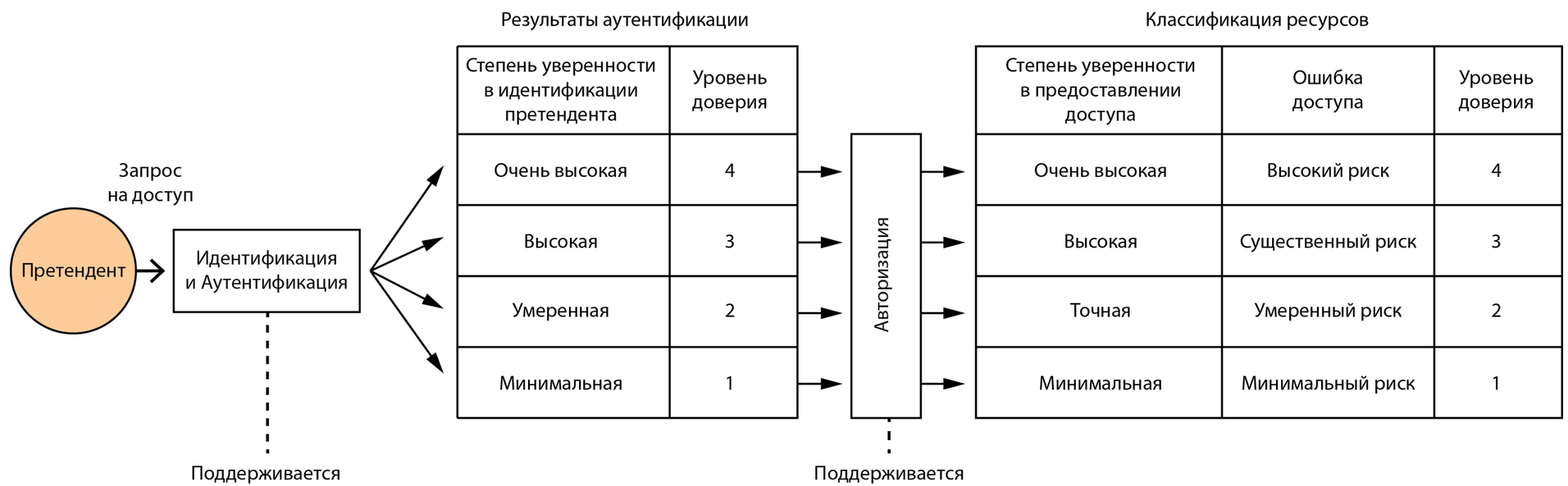
Актуальные проблемы стандартизации по управлению доступом и защите персональных данных

Рускрипто

25 марта 2021 г.

Алексей Сабанов, д.т.н.,
Эксперт ISO/JTC1/SC27/WG5
Член ТК-362, ТК-122,
доцент МГТУ им. Баумана
Зам. ген. директора ЗАО "Аладдин Р.Д."

Уровни доверия: доступ к онлайн - транзакциям



ISO/IEC 29146:2016

Цели идентификации и аутентификации

Цель первичной идентификации – проверка и подтверждение того, что субъект является тем, за кого себя выдает (задача распознания).

Первичная идентификация является основным и самым сложным этапом регистрации нового пользователя в информационной системе. Итогом первичной регистрации является появление новой учетной записи и присвоением субъекту доступа уникального идентификатора, чтобы отличать его от других пользователей данной ИС. Учетная запись содержит идентификатор, зарегистрированные методы аутентификации (как правило, основной и запасной), соответствующие им секреты (аутентификационную информацию или сведения о ее применении – в случае закрытого ключа доступа), а также присоединенную идентификационную информацию (в том числе биометрию и процесс её снятия для получения качественного образца, в том числе для неотказуемости регистрации - Non repudiation).

Вторичная идентификация (многократно воспроизводится при каждой попытке доступа) – процедура опознания «своего» из множества зарегистрированных пользователей.

Цель аутентификации – проверка знания субъектом своего идентификатора и проверка владения субъектом аутентификационной информацией (одним или несколькими зарегистрированными аутентфикаторами), подтверждающей то, что он является тем ЗАРЕГИСТРИРОВАННЫМ в ИС пользователем, за кого себя выдает. По сути аутентификация должна ответить на вопрос о степени уверенности в том, идентичен ли заявитель ранее аутентифицированному пользователю (ISO/IEC 29115, последняя редакция).

Характеристики доверия к результату первичной идентификации

Первичная регистрация субъекта (объекта) доступа			Допущения, определяемые правилами управления доступом	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
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

Общая характеристика доверия к результатам идентификации

Первичная идентификация субъекта (объекта) доступа			Вторичная идентификация субъекта (объекта) доступа	Уверенность в том, что субъект (объект) доступа соответствует идентификационной информации	Уровень доверия к результатам идентификации субъекта (объекта) доступа
Соответствие заявленных идентификационных данных требованиям к первичной идентификации	Подтверждение заявленных идентификационных данных	Возможность регистрация субъекта (объекта) доступа			
Не соответствуют	–	Отказ в регистрации субъекта доступа	–	–	–
Не соответствуют	Не подтверждаются	Регистрация субъекта доступа как «анонима»	Выполнена успешно	Нет уверенности	Нет
Соответствуют	Не подтверждаются	Регистрация субъекта доступа	Выполнена успешно	Некоторая уверенность	Низкий уровень доверия
Соответствуют	Подтверждаются	Регистрация субъекта доступа	Выполнена успешно	Умеренная уверенность	Средний уровень доверия
Соответствуют	Подтверждаются официально	Регистрация субъекта доступа	Выполнена успешно	Высокая уверенность	Высокий уровень доверия

Оценка доверия к результатам первичной идентификации

Уровень доверия к первичной идентификации (ПИ) субъекта можно оценить с помощью обобщенной безразмерной функции доверия $\boldsymbol{\psi}_{\text{ПИ}}$, область изменений которой ограничена: $0 \leq \boldsymbol{\psi}_{\text{ПИ}} < 1$.

В формализованном виде $\boldsymbol{\psi}_{\text{ПИ}}$ можно представить в виде:

$$\boldsymbol{\psi}_{\text{ПИ}} = \boldsymbol{\psi}_{\text{уник.}} \cap \boldsymbol{\psi}_{\text{подтвержд.}} \cap \boldsymbol{\psi}_{\text{прив.}}, \qquad (1)$$

где $\boldsymbol{\psi}_{\text{уник.}}$ – безразмерная функция, характеризующая уровень доверия к уникальности совокупности предъявленных идентификационных атрибутов;

$\boldsymbol{\psi}_{\text{подтвержд.}}$ - безразмерная функция, характеризующая уровень доверия к результатам верификации предъявленных идентификационных атрибутов;

$\boldsymbol{\psi}_{\text{прив.}}$ - безразмерная функция, характеризующая уровень доверия к результатам привязки верифицированных идентификационных атрибутов к личности заявителя.

Оценка доверия к результатам ПИ

Уровень доверия к результатам первичной идентификации субъекта доступа может быть оценена не только на основе анализа процессов, но и по показателям надежности, достоверности и выполнения требований безопасности:

$$\boldsymbol{\psi}_{\text{ПИ}} = \boldsymbol{\psi}_{\text{надежн.}} \cap \boldsymbol{\psi}_{\text{дост.}} \cap \boldsymbol{\psi}_{\text{безоп.}}, \qquad (2)$$

где $\boldsymbol{\psi}_{\text{надежн.}}$ – безразмерная характеристика надежности ПИ;
$\boldsymbol{\psi}_{\text{дост.}}$ – безразмерная характеристика достоверности ПИ;
$\boldsymbol{\psi}_{\text{безоп.}}$ – безразмерная характеристика выполнения требований информационной безопасности, в частности, защиты персональных данных субъектов доступа согласно требованиям Федерального закона 152-ФЗ.
При выполнении оценок по формулам (1) и (2) в дальнейшие расчеты выбирается минимальное из полученных значений $\boldsymbol{\psi}_{\text{ПИ}}$.

Общая характеристика уровней доверия к результатам аутентификации по методам аутентификации

Метод аутентификации субъекта (объекта) доступа			Вид аутентификации субъекта (объекта) доступа	Уверенностью в том, что субъект и (или) объект доступа действительно является тем зарегистрированным субъектом (объектом) доступа, за кого себя выдает	Уровень доверия к результатам аутентификации субъекта (объекта) доступа
Однофакторная аутентификация	Односторонняя аутентификация	Соответствующие протоколы аутентификации, в том числе и криптографические	Простая	Некоторая уверенность	Низкий уровень доверия
Многофакторная аутентификация	Односторонняя или взаимная аутентификация	Соответствующие протоколы аутентификации, в том числе и криптографические	Усиленная	Умеренная уверенность	Средний уровень доверия
Многофакторная аутентификации	Взаимная аутентификация	Криптографические протоколы аутентификации	Строгая	Высокая уверенность	Высокий уровень доверия

Уровни доверия к методам аутентификации

№	Что используется при аутентификации	Аутентификационная информация	Защита аутентификационной информации	Обмен	Факторы аутентификации	Вид аутентификации	Уровень доверия к результату аутентификации
1	запоминаемый секрет (примеры: пароль, PIN-код)	пароль	защита пароля от атак	односторонний	знание	простая	низкий
2	сгенерированный заранее одноразовый пароль, записанный на носителе (пример: скрэтч-карта)	одноразовый пароль	доверенный ДСЧ, защита канала распределения OTP, защита от MitM-атак	односторонний	владение		
3	"второй канал" (пример: телефон+SMS)	одноразовый пароль	защита операций аутентификации в обоих каналах	односторонний	владение		средний
4	устройство одноразовых паролей, динамически генерирующая OTP	одноразовый пароль	защита устройства	односторонний	владение		
5	многоразовый пароль + устройство OTP	одноразовый пароль + многоразовый пароль	защита многоразового пароля от атак	односторонний	владение + знание	усиленная	высокий
6	многоразовый пароль + устройство OTP с доступом к устройству по паролю или биометрии	одноразовый пароль + многоразовый пароль	защита устройства и многоразового пароля	односторонний	владение + знание или биометрия		
7	криптографическй ключ в СВТ или на незащенном паролем носителе	криптографические ключи	защита ключей	односторонний или взаимный	владение		
8	устройство (СВТ или смартфон) с криптографическим ПО + доступ к ключу по паролю	криптографические ключи	защита устройства	односторонний или взаимный	владение + знание		
9	СВТ с криптографическим ПО + доступ к ключу по паролю	криптографические ключи	защита ключей	взаимный	владение + знание	строгая	очень высокий
10	СВТ с криптографическим ПО и отдельное устройство с помещённым и хранящемся в нём криптографическим ключом + доступ к ключу по паролю или биометрии	криптографические ключи	защита устройства, содержащего ключ	взаимный	владение + знание или биометрия		
11	СВТ с криптографическим ПО и отдельное устройство с криптографическим ПО, генерирующее неизвлекаемые ключи (SSCD) + доступ к ключу по паролю и/или биометрии	криптографические ключи	защита устройства, содержащего ключ	взаимный	владение + знание и/или биометрия		самый высокий

Оценка доверия к результатам аутентификации

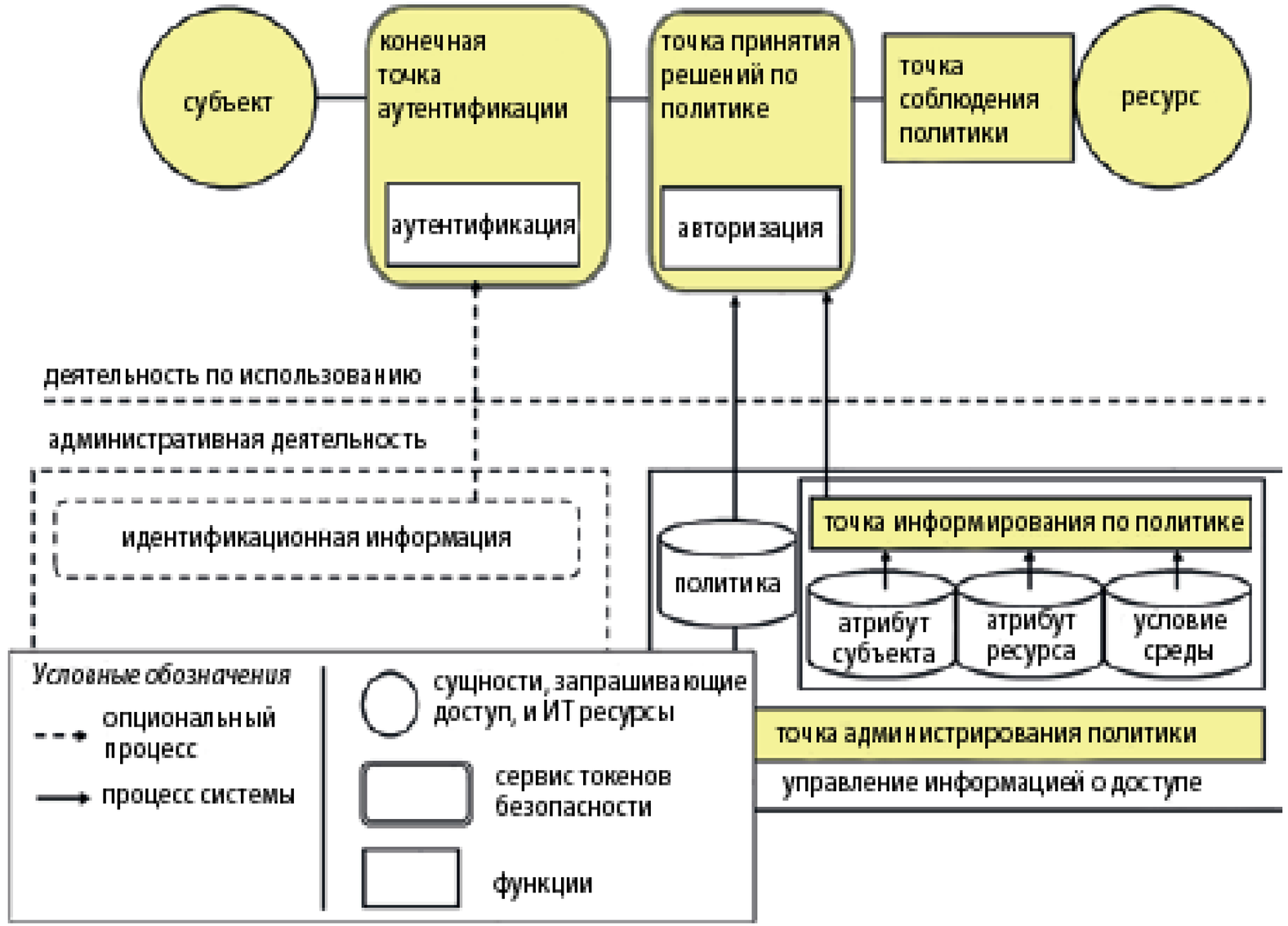
Оценка уровня доверия к результатам аутентификации субъекта доступа также может быть выражена через обобщенную безразмерную функцию доверия $\boldsymbol{\psi}_{\text{аут.}}$:

$$\boldsymbol{\psi}_{\text{аут.}} = \boldsymbol{\psi}_{\text{ПИ}} \cap \boldsymbol{\psi}_{\text{метод}} \cap \boldsymbol{\psi}_{\text{секр.}}, \quad (3)$$

где $\boldsymbol{\psi}_{\text{метод}}$ – безразмерная функция, характеризующая уровень доверия к используемому методу аутентификации, определяемому количеством применяемых факторов аутентификации, способом обмена аутентификационной информацией (односторонний или взаимный) и применяемыми протоколами аутентификации,

$\boldsymbol{\psi}_{\text{секр.}}$ – безразмерная функция, характеризующая средства аутентификации, определяемых способом генерации, хранения и применения секрета, используемого в качестве аутентифицирующей информации.

Схема управления санкционированным доступом



Оценка доверия к работе системы управления доступом

С учетом соотношений (1) – (3) результирующий уровень доверия к результатам функционирования СУЛД можно оценить с помощью обобщенной безразмерной функции доверия $\boldsymbol{\psi}_{\text{рез}}$:

$$\boldsymbol{\psi}_{\text{рез.}} = \boldsymbol{\psi}_{\text{аут.}} \cap \boldsymbol{\psi}_{\text{УП}} \cap \boldsymbol{\psi}_{\text{МРД}} \cap \boldsymbol{\psi}_{\text{СП}} \cap \boldsymbol{\psi}_{\text{МА}}, \qquad (4)$$

где $\boldsymbol{\psi}_{\text{СП}}$ – безразмерная характеристика соблюдения политики,
$\boldsymbol{\psi}_{\text{УП}}$ – безразмерная характеристика качества управления привилегиями;
$\boldsymbol{\psi}_{\text{МРД}}$ – безразмерная характеристика реализации модели разделения доступа;
$\boldsymbol{\psi}_{\text{МА}}$- безразмерная характеристика качества мониторинга и аудита.
Чтобы результирующий уровень доверия был достаточно высоким, все составляющие должны быть «равнопрочными» и как можно близкими к значению единицы.

Проблема стандартизации по защите ПДн

1. ISO/IEC 29100:2011 Privacy framework – Руководство по защите ПДн - ЕСТЬ в РФ
2. ISO/IEC 29101:2018 Privacy architecture framework – Руководство по архитектуре защиты ПДн
3. ISO/IEC 29134:2017 PIA Guiderlines
4. ISO/IEC 29151 PII protection – защита идентифицирующей информации
5. ISO/IEC 29184 Online privacy notices and consent – Он-лайн уведомление о согласии [на обработку] и конфиденциальности ПДн.
6. ISO/IEC 29190:2015 Privacy capability assessment model - Модель утверждений, способная обеспечить защиту ПДн
7. ISO/IEC 29191:2012 Anonymous protection - Requirements for partially anonymous, partially unlinkable authentication – Защита информации анонимного пользователя – Требования к аутентификации частично не идентифицированного, частично не связанного [с поставщиком идентификационных услуг] пользователя
8. ISO/IEC 27017 Практические правила защиты ПДн в публичных облаках (на основе 27002)
9. ISO/IEC 27550:2019 Privacy Engineering – Разработка защиты ПДн
10. ISO/IEC 27551:-в разработке Requirements for attribute-based unlinkable entity authentication – Требования к аутентификации сущности на основе несвязанных атрибутов
11. ISO/IEC 27552:-в разработке Extension 27001 for privacy information management -Расширение стандарта 27001 на управление персональной информацией
12. ISO/IEC 27570:-в разработке Privacy for smart cities
13. ISO/IEC 29556:-в разработке User-centric framework for PII handling based on privacy preferences
14. ISO/IEC 27018 Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors – Свод правил защиты ПДн в публичных облаках, выполняющих функции процессоров идентификации личности
15. ISO/IEC 27570 Privacy for smart cities – Защита ПДн в «умных городах»
16. ISO/IEC 20889 Privacy enhancing data deidentification terminology and classification of techniques – Терминология и классификация технологий усиления обезличивания персональных данных
17. ISO/IEC 20547-4 Big data sensitivity and privacy – Чувствительность и приватность больших данных (Big data)
18. ISO/IEC 20649:-в разработке Privacy enhancing data de-identification
19. ISO/IEC 22307:2008 Privacy impact assessment
20. ISO/IEC 19092: 2008 Financial services-Biometrics – Security framework

Проблема стандартизации по применению биометрии

- Во всемирной организации по стандартизации имеется 37-й подкомитет первого комитета по разработке стандартов ИТ с применением биометрии ISO/IEC JTC 1/SC 37 (биометрия), также интенсивно работает SC 17 (смарт-карты и приватная информация)
- Приказом Росстандарта № 624 от 20.05.2014 (утратил силу, теперь это Приказ № 448 от 06.03.2017) в 2014 г. создан ТК-098, в сферу задач которого входит ОКПД 71.90.15 «Услуги консультативные по вопросам обеспечения безопасности», а также мониторинг и оценка уязвимостей транспортных систем.
- На сайте ТК-098 «Биометрия и биомониторинг» в списке 46 действующих стандартов по биометрии, среди них отсутствуют более 15 стандартов по безопасности применения биометрии
- В то же время в системе ISO/IEC принято 10 и находится в разработке 6 новых и в стадии пересмотра 5 стандартов. Пересмотр касается новых технологий и учета положений ISO 27XXX (управление безопасностью) и ISO 31XXX (управление рисками)

Стандарты ISO по безопасности применения биометрии

1. ISO/IEC 17922:2017 Information technology—Security techniques — Telebiometric authentication framework using biometric hardware security module
2. ISO 19092:2008, Financial services — Biometrics —Security framework
3. ISO/IEC 19792:2009, Information technology — Security techniques — Security evaluation of biometrics
4. ISO/IEC 24761:2009, Information technology — Security techniques — Authentication context for biometrics
5. ISO/IEC 19989, Information technology — Security techniques — Criteria and methodology for security evaluation of biometric systems All 4 parts
6. ISO/IEC/TR 29156:2015, Information technology — Guidance for specifying performance requirements to meet security and usability needs in applications using biometrics
7. ISO/IEC 29115:2013, Information technology — Security techniques — Entity authentication assurance framework
8. ISO/IEC 29144:2014 Information technology — Biometrics — The use of biometric technology in commercial Identity Management applications and processes
9. ISO/IEC 30136:2018 Information technology — Performance testing of biometric template protection schemes
10. ISO/IEC 19989-1:2020, Information Technology — Security techniques — Criteria and methodology for security evaluation of biometric systems – Part 1: framework
11. ISO 12812-1, Core banking — Mobile financial services — Part 1: General framework
12. ISO/IEC 24714-1 Information technology — Biometrics — Jurisdictional and societal considerations for commercial applications — Part 1
13. ISO/IEC TR 24741, Information technology — Biometrics tutorial
14. ISO/IEC 24745, Information technology — Security techniques — Biometric information protection
15. ISO/IEC 27553 Information technology — Security techniques —Security requirements for authentication using biometrics on mobile devices
16. ISO/IEC 27555 Performance testing of biometric template protection schemes
17. ISO/IEC 30107, Information technology — Biometric presentation attack detection (All parts)
18. ISO/IEC TR 30125, Information technology — Biometrics used with mobile devices

Общий анализ стандартов ISO по биометрии+ИБ

- В стандартах приведены рекомендации по обращению с биометрическими персональными данными (ISO 19792:2009, ISO/IEC 24745, ISO/IEC 19989), в финансовой сфере – ISO 19092:2008
- Рассмотрены типовые архитектурные решения по применению биометрии в мобильных устройствах - ISO/IEC 17922:2017, ISO/IEC 27553, ISO/IEC TR 30125
- Показана необходимость учета рисков (атака на биометрические данные, PAD, отказ от регистрации легального пользователя, подмена сервера, подмена мобильного приложения, доступ к биометрическим данным неуполномоченного лица и др.) для работы ИС (приемлемый уровень рисков, методы управления рисками – ISO/IEC 27553.
- Приводятся:
  - самая безопасная схема применения - биометрия сравнивается по принципу 1:1 прямо на мобильном устройстве внутри TEE (Trusted execution environment) для доступа к закрытому ключу, который является аутентифицирующей информацией - ISO/IEC 17922;
  - Самая опасная схема – биометрия сравнивается на сервере и участвует в аутентификации – ISO/IEC 27553.

Спасибо за внимание!

Тел. 8-985-924-52-09,
a.sabanov@aladdin-rd.ru