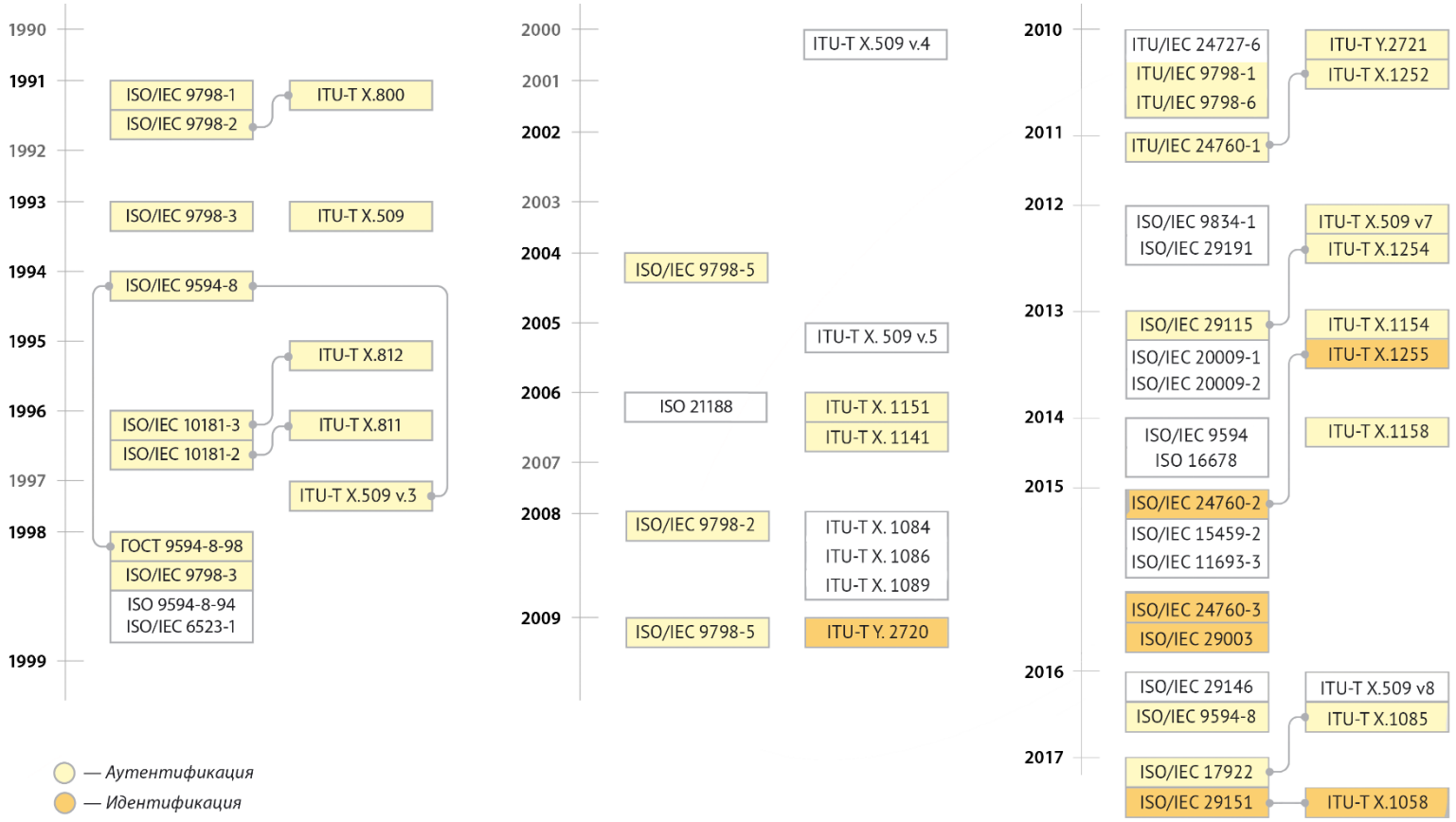
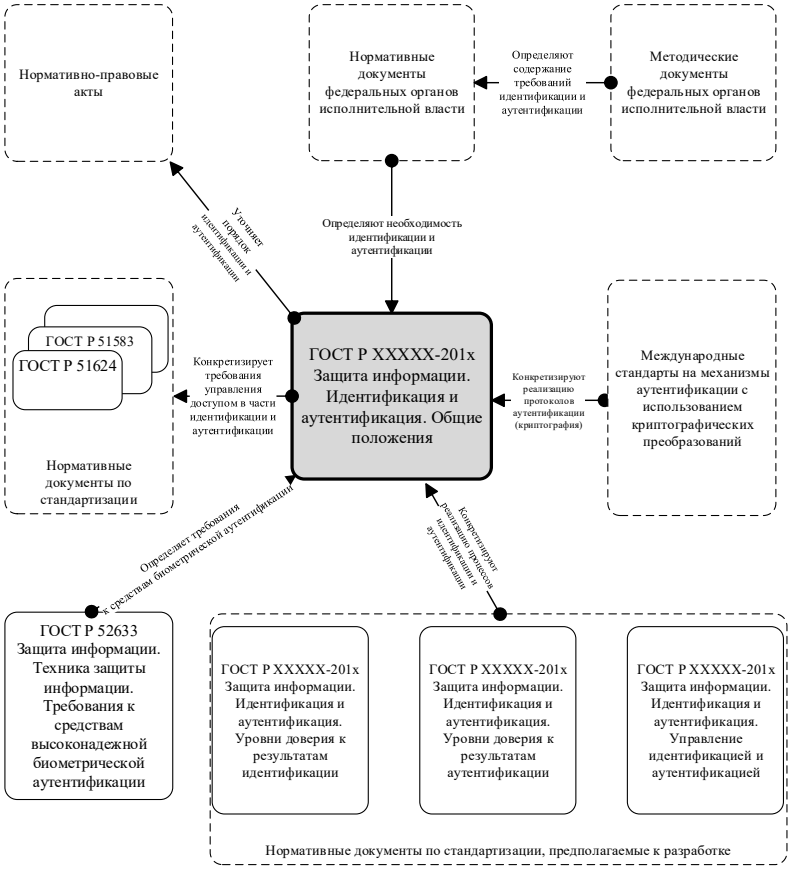
ГОСТ Р «Идентификация и аутентификация. Общие положения» и ГОСТ Р «Уровни доверия к результатам идентификации». Стандарты ISO в области идентификации и аутентификации, а также защиты персональных данных

Сабанов Алексей Геннадьевич,
к.т.н., доцент МГТУ им. Баумана,
Эксперт ISO/C1/SC27/WG5,
Член ТК 362, ТК 26, ТК 122
Зам. ген. директора ЗАО "Аладдин Р.Д."

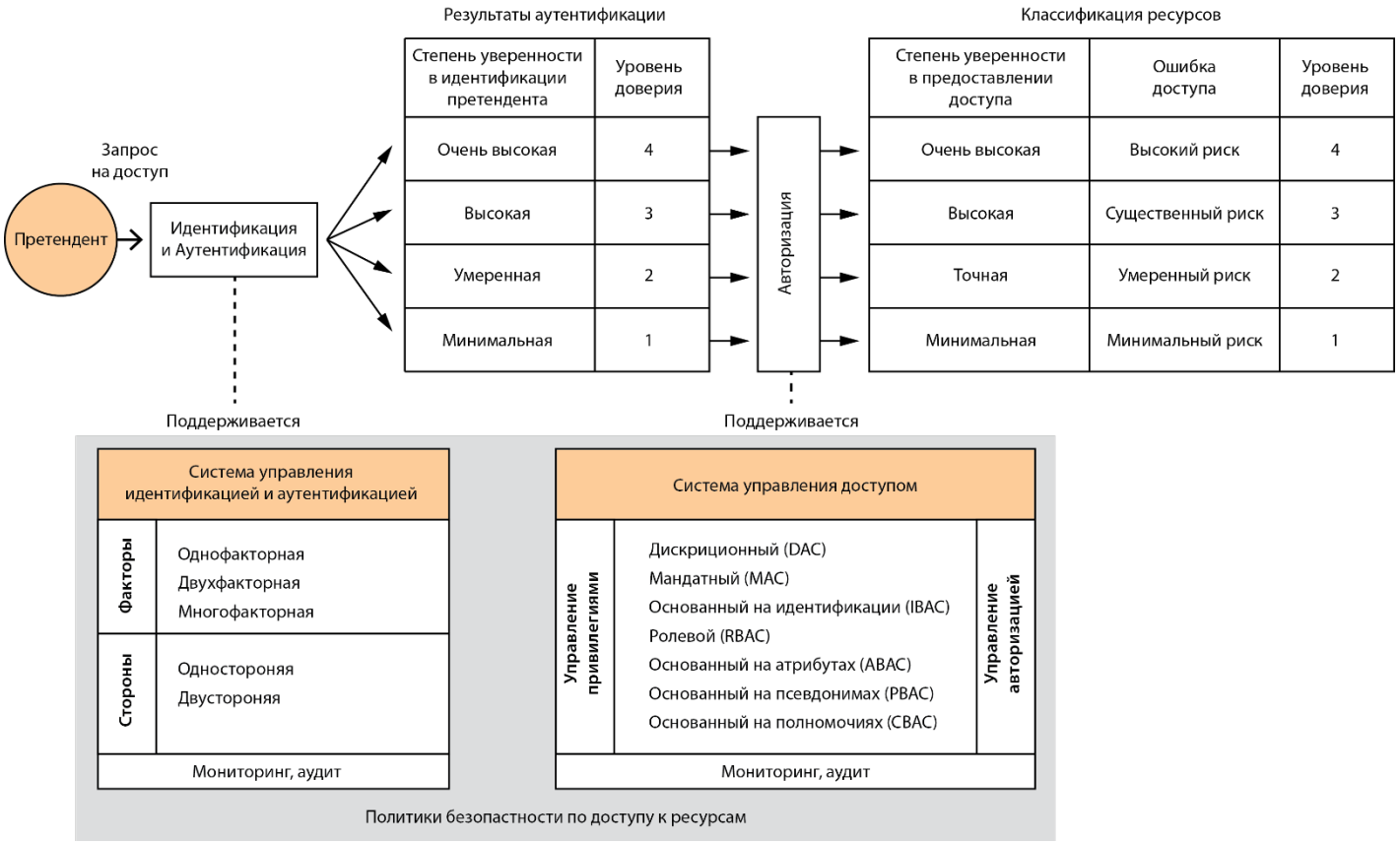
Стандарты по идентификации и аутентификации



План по развитию системы национальных стандартов



Взаимосвязь уровней доверия: доступ к транзакциям



ISO/IEC 29146:2016

Рабочая группа WG5

- Identification
- Authentication
- Access control (IDm framework, Role-based and attribute-based access control)
- Biometrics
- Privacy framework

В работе в настоящее время

- ISO/IEC 29115-2013 Entity authentication assurance
- ISO/IEC 9798-2 – (2016) Entity authentication
- ISO/IEC 27551 Requirements for attribute-based unlinkable entity authentication
- ISO/IEC 29191

- ISO/IEC 29003-2017 Identity proofing
- ISO/IEC 24760-1 Identity
- ISO/IEC 24760-2 Identity
- ISO/IEC 24760-3 Identity
- ISO/IEC 24761 IDm Systems
- Application of ISO 31000 for identity-related risks
- Application of ISO 27000 for identification and authentication

Защита персональных данных

- ISO/IEC 29100 Privacy framework
- ISO/IEC 29101 Privacy architecture framework
- ISO/IEC 29190 Privacy capability assessment model
- ISO/IEC 27550 Privacy Engineering
- ISO/IEC 29191 Anonymous protection - Requirements for partially anonymous, partially unlinkable authentication
- ISO/IEC 27018 Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors
- ISO/IEC 29151 PII protection
- ISO/IEC 27570 Privacy for smart cities
- ISO/IEC 20889 Privacy enhancing data de-identification techniques
- ISO/IEC 20547-4 Big data sensitivity and privacy
- ISO/IEC 29184 Online privacy notices and consent

Биометрия в идентификации

- Биометрия используется только в дополнение к другим идентификационным атрибутам (паспорт, СНИЛС, ИНН,…). «Биометрическое распознавание не может использоваться изолированно или вместо верификации других идентифицирующих атрибутов» - ISO/IEC 29003, раздел B4.
- Биометрия может использоваться для предотвращения дублирования записи, связанной с конкретным субъектом, в реестре (сравнение биометрического образца субъекта с другими биометрическими образцами. Собранная биометрическая информация должна быть достаточной и эффективной для исключения дублирования идентификационных данных - ISO/IEC 29003 29003, п.4.8)
- **Противодействие попыткам множественной регистрации**.
- Подтверждение идентификационных данных
- Неотказуемость от регистрации нового пользователя ИС
- *Установление привязки идентификационной информации к конкретной личности*: привязка устанавливается путем сопоставления биологической или поведенческой характеристики, наблюдаемой подтверждающей стороной, с эталонной биометрической информацией, которая, как известно, соответствует субъекту - ISO/IEC 29003, разд. 5.5

Биометрия в аутентификации

- Биометрический фактор должен использоваться только совместно с другими факторами, в том числе для подтверждения фактора владения - ISO/IEC 29003, раздел B.4. Например, стандарт США FIPS Pub 201-2 рекомендует использовать биометрию (отпечаток пальца) для разблокирования смарт-карты государственных служащих.
- Термин «биометрическая аутентификация» обычно применяется только при сравнении 1:1, например, в технологии Match on Card. «Биометрическая аутентификация обычно включает сравнение вида «один к одному» полученного от субъекта биометрического образца с хранящимся биометрическим эталоном для заявленных субъектом идентификационных данных». – ISO/IEC 29003, раздел B.4, NIST SP 800-63B.
- Применение биометрических характеристик в качестве единственного фактора при однофакторной аутентификации не допускается (Вероятность взлома биометрических систем в процессе сбора данных, особенно при удаленном сборе биометрических данных с использованием ненадежных сетей) - User Authentication Guidance for Information Technology Systems/ ITSP.30.031 V3 April 2018
- Биометрический фактор всегда имеет вероятностную природу, в отличие от детерминированных стандартных аутентифицирующих данных (пароль, ОТП, закрытый ключ). Поэтому применение биометрии в аутентификации ограничивается подтверждением, например, фактора владения смарт-картой, токеном, etc.

Спасибо за внимание!

asabanov@mail.ru
+7-985-924-52-09