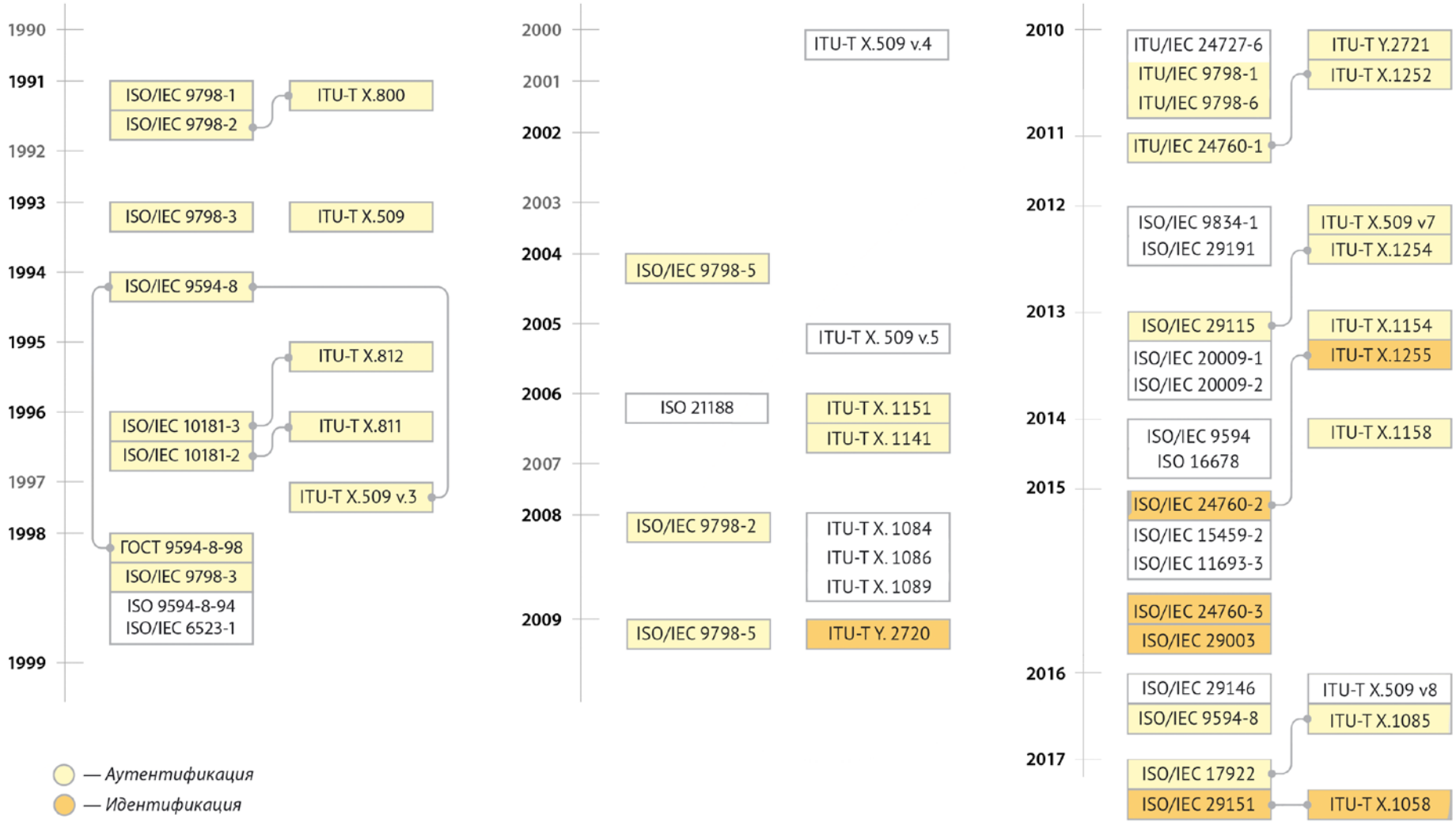
Вопросы идентификации и аутентификации в информационных и автоматизированных системах

ТБ – форум
13 февраля 2019 г.

Сабанов А.Г., к.т.н.,
Член ТК-362, ТК-122,
Заместитель генерального
Директора ЗАО «Аладдин Р.Д.»

Международные стандарты по идентификации и аутентификации



Определения

Идентификация – действия по присвоению субъектам и объектам доступа идентификаторов и (или) по сравнению предъявляемого идентификатора с перечнем присвоенных идентификаторов. Идентификатор: Признак субъекта доступа или объекта доступа в виде строки знаков (символов), который используется при идентификации и однозначно определяет (указывает) соотнесенную с субъектом идентификационную информацию. Атрибут: характеристика или свойство субъекта или объекта доступа.

Аутентификация – действия по проверке подлинности субъекта доступа и/или объекта доступа, а также по проверке принадлежности субъекту доступа (объекту доступа) предъявленного идентификатора доступа и аутентификационной информации.

Факторы аутентификации - вид (форма) существования аутентификационной информации, предъявляемой субъектом доступа при аутентификации:

- фактор знания: субъект доступа должен знать что-то определенное (например, аутентификационную информацию в виде пароля, PIN-кода и т. п.);

фактор владения: субъект доступа должен обладать чем-то определенным (например, устройством, содержащим аутентификационную информацию);

фактор биометрический: субъекту доступа должно быть свойственно что-то определенное (например, биометрические данные физического лица или шаблон поведения).

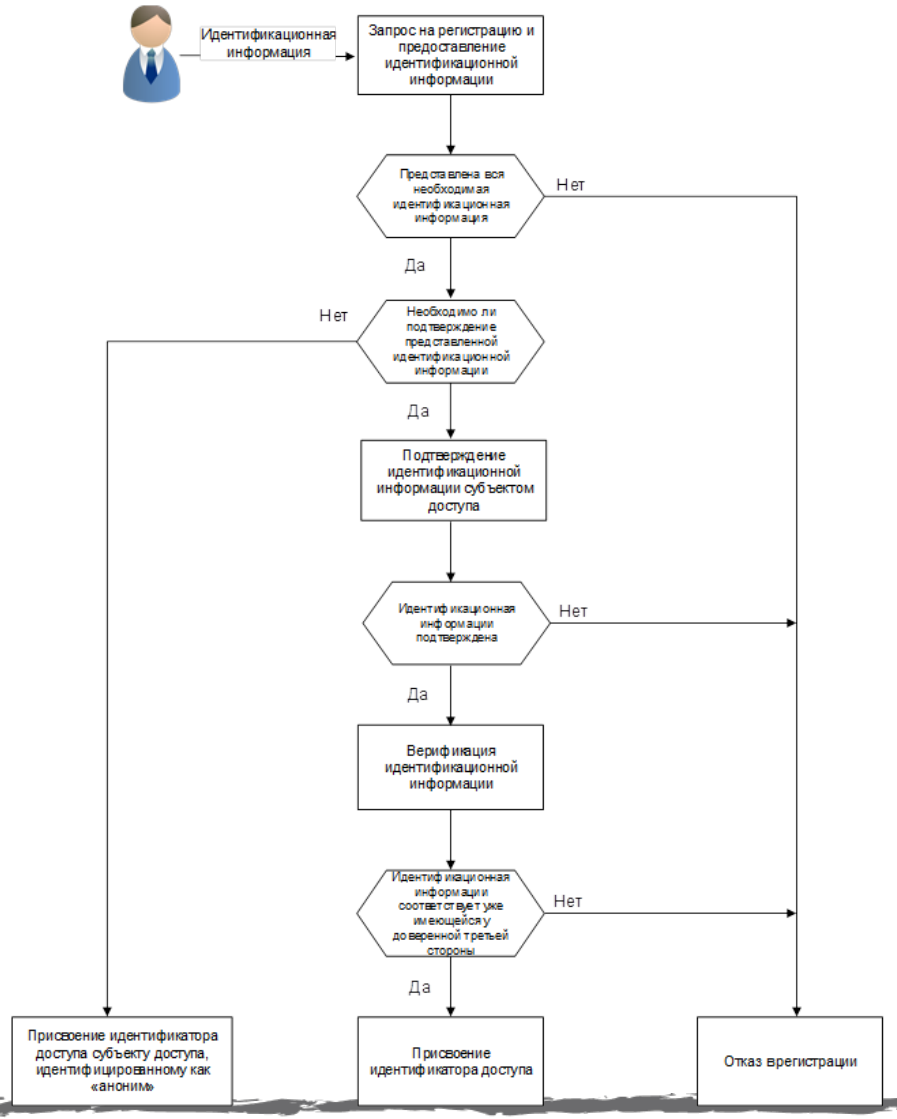
Проект ГОСТ Р Идентификация и аутентификация. Общие положения

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.

Минимально достаточный объем и уникальность идентификационной информации, связанной с субъектом (объектом) доступа, а также оценка и подтверждение идентификационных данных по установленным правилам должны обеспечить необходимую уверенность в том, что заявленные идентификационные данные действительно соответствуют данному субъекту (объекту) доступа.

Схема первичной идентификации



Первичная идентификация

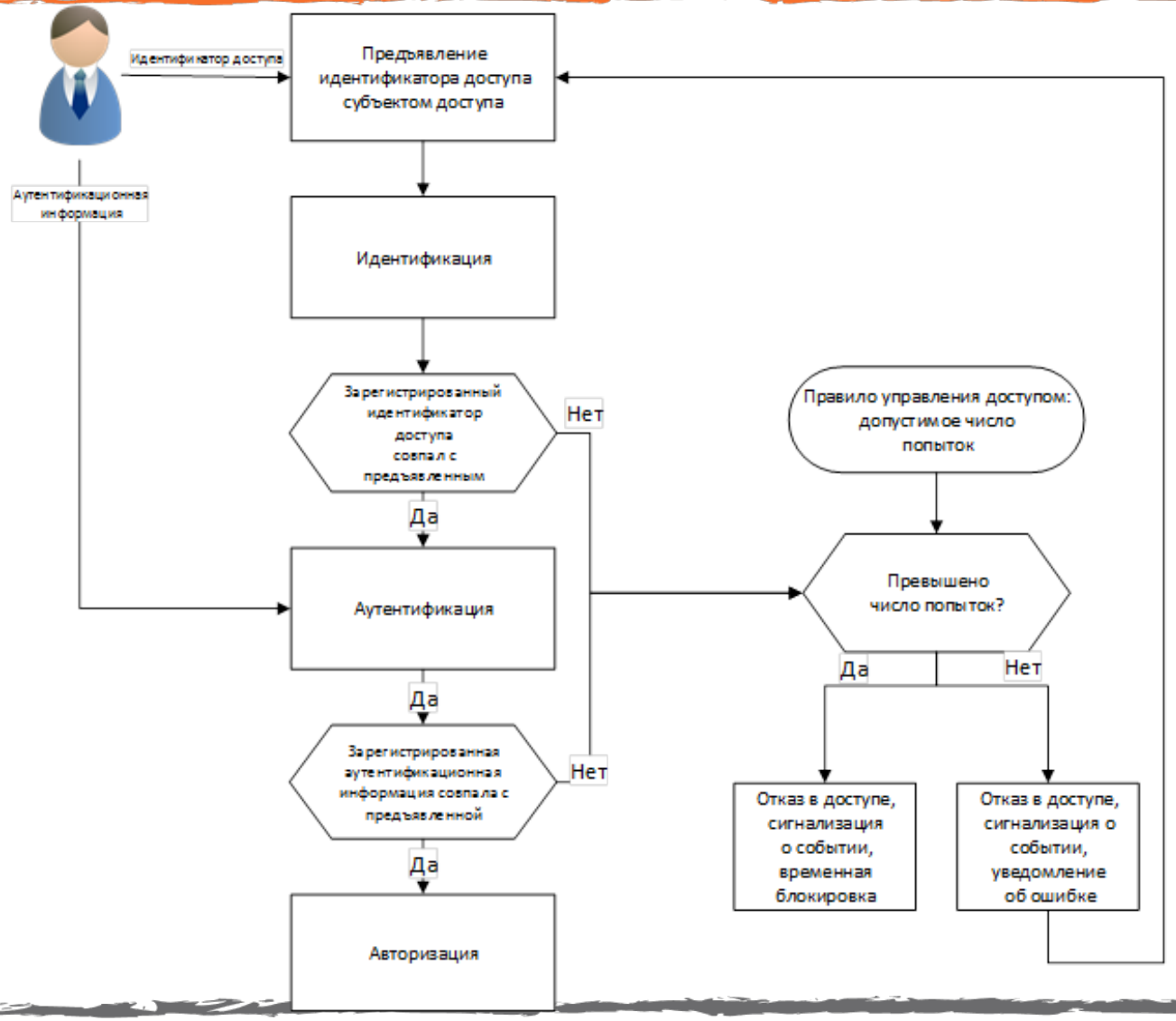
Целью первичной идентификации является установление (подтверждение) соответствия между субъектом доступа и заявленными им идентификационными данными.

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.

Схема вторичной идентификации и аутентификации



ISO/IEC 29003 Уровни подтверждения идентификационных данных

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 Существование e-Id и связка идентификационных данных с личностью заявителя

	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 привязке данных к субъекту

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.

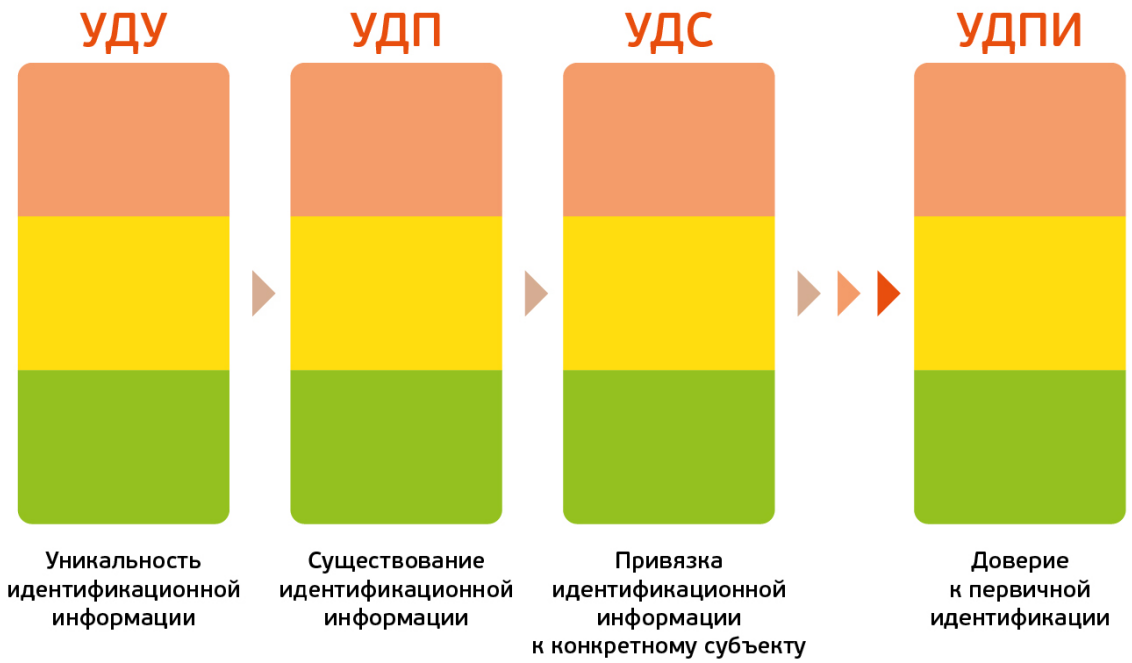
Общая характеристика доверия к результатам первичной идентификации

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

Формирование уровней доверия к результатам первичной идентификации



Общая характеристика уровней доверия к результатам 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 результатам аутентификации

№	Что используется при аутентификации	Аутентификационная информация	Защита аутентификационной информации	Обмен	Факторы аутентификации	Уровень доверия к результату аутентификации
1	запоминаемый секрет (примеры: пароль, PIN-код)	пароль	защита пароля от известных атак	односторонний	знание	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	
4	устройство одноразовых паролей, динамически генерирующая OTP	одноразовый пароль	защита устройства	односторонний	владение	
5	многоразовый пароль + устройство OTP+ доступ к устройству по паролю или биометрии	многоразовый пароль + одноразовый пароль + пароль на доступ к устройству	защита устройства и многоразового пароля	односторонний	владение + знание или биометрия	высокий
6	средство СВТ + криптографическое ПО	криптографические ключи	защита ключей	односторонний или взаимный	владение	
7	устройство (смартфон) + криптографическое ПО + доступ к ключу по паролю	криптографические ключи	защита устройства	односторонний или взаимный	владение + знание	
8	СВТ + криптографическое ПО + доступ к ключу по паролю	криптографические ключи	защита ключей	взаимный	владение + знание	очень высокий
9	СВТ + отделённое устройство с криптографией + доступ к устройству по паролю или биометрии	криптографические ключи	защита устройства, содержащего ключ	взаимный	владение + знание или биометрия	
10	СВТ + отделённое устройство, генерирующее неизвлекаемые ключи (SSCD) с криптографией + доступ к устройству по паролю или биометрии	криптографические ключи	защита устройства, содержащего ключ	взаимный	владение + знание и/или биометрия для доступа к криптографическому ключу	

Доверие к результатам идентификации и аутентификации

	Низкий уровень доверия к результатам идентификации	Средний уровень доверия к результатам идентификации	Высокий уровень доверия к результатам идентификации
Низкий уровень доверия к результатам аутентификации	Низкий уровень доверия	Низкий уровень доверия	Низкий уровень доверия
Средний уровень доверия к результатам аутентификации	Низкий уровень доверия	Средний уровень доверия	Средний уровень доверия
Высокий уровень доверия к результатам аутентификации	Низкий уровень доверия	Средний уровень доверия	Высокий уровень доверия