Международный союз электросвязи

МСЭ-Т

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

X.1254

(09/2020)

СЕРИЯ X: СЕТИ ПЕРЕДАЧИ ДАННЫХ,
ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ
И БЕЗОПАСНОСТЬ

Безопасность киберпространства –
Управление определением идентичности

Структура гарантии аутентификации объекта

Рекомендация МСЭ-Т X.1254

ITU-T

Международный союз электросвязи

РЕКОМЕНДАЦИИ МСЭ-Т СЕРИИ X

СЕТИ ПЕРЕДАЧИ ДАННЫХ, ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ И БЕЗОПАСНОСТЬ

СЕТИ ПЕРЕДАЧИ ДАННЫХ ОБЩЕГО ПОЛЬЗОВАНИЯ	X.1–X.199
ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ	X.200–X.299
ВЗАИМОДЕЙСТВИЕ МЕЖДУ СЕТЯМИ	X.300–X.399
СИСТЕМЫ ОБРАБОТКИ СООБЩЕНИЙ	X.400–X.499
СПРАВОЧНИК	X.500–X.599
ОРГАНИЗАЦИЯ СЕТИ ВОС И СИСТЕМНЫЕ АСПЕКТЫ	X.600–X.699
УПРАВЛЕНИЕ В ВОС	X.700–X.799
БЕЗОПАСНОСТЬ	X.800–X.849
ПРИЛОЖЕНИЯ ВОС	X.850–X.899
ОТКРЫТАЯ РАСПРЕДЕЛЕННАЯ ОБРАБОТКА	X.900–X.999
БЕЗОПАСНОСТЬ ИНФОРМАЦИИ И СЕТЕЙ	
Общие аспекты безопасности	X.1000–X.1029
Безопасность сетей	X.1030–X.1049
Управление безопасностью	X.1050–X.1069
Телебиометрия	X.1080–X.1099
БЕЗОПАСНЫЕ ПРИЛОЖЕНИЯ И УСЛУГИ (1)	
Безопасность многоадресной передачи	X.1100–X.1109
Безопасность домашних сетей	X.1110–X.1119
Безопасность подвижной связи	X.1120–X.1139
Безопасность веб-среды	X.1140–X.1149
Протоколы безопасности (1)	X.1150–X.1159
Безопасность одноранговых сетей	X.1160–X.1169
Безопасность сетевой идентификации	X.1170–X.1179
Безопасность IPTV	X.1180–X.1199
БЕЗОПАСНОСТЬ КИБЕРПРОСТРАНСТВА	
Кибербезопасность	X.1200–X.1229
Противодействие спаму	X.1230–X.1249
Управление определением идентичности	**X.1250–X.1279**
БЕЗОПАСНЫЕ ПРИЛОЖЕНИЯ И УСЛУГИ (2)	
Связь в чрезвычайных ситуациях	X.1300–X.1309
Безопасность повсеместных сенсорных сетей	X.1310–X.1319
Безопасность "умных" электросетей	X.1330–X.1339
Сертифицированная электронная почта	X.1340–X.1349
Безопасность интернета вещей (IoT)	X.1360–X.1369
Безопасность интеллектуальных транспортных систем (ИТС)	X.1370–X.1389
Безопасность технологии распределенного реестра	X.1400–X.1429
Безопасность технологии распределенного реестра	X.1430–X.1449
Протоколы безопасности (2)	X.1450–X.1459
ОБМЕН ИНФОРМАЦИЕЙ, КАСАЮЩЕЙСЯ КИБЕРБЕЗОПАСНОСТИ	
Обзор кибербезопасности	X.1500–X.1519
Обмен информацией об уязвимости/состоянии	X.1520–X.1539
Обмен информацией о событии/инциденте/эвристических правилах	X.1540–X.1549
Обмен информацией о политике	X.1550–X.1559
Эвристические правила и запрос информации	X.1560–X.1569
Идентификация и обнаружение	X.1570–X.1579
Гарантированный обмен	X.1580–X.1589
БЕЗОПАСНОСТЬ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ	
Обзор безопасности облачных вычислений	X.1600–X.1601
Проектирование безопасности облачных вычислений	X.1602–X.1639
Передовой опыт и руководящие указания в области облачных вычислений	X.1640–X.1659
Обеспечение безопасности облачных вычислений	X.1660–X.1679
Другие вопросы безопасности облачных вычислений	X.1680–X.1699
КВАНТОВАЯ СВЯЗЬ	
Терминология	X.1700–X.1701
Квантовый генератор случайных чисел	X.1702–X.1709
Структура безопасности QKDN	X.1710–X.1711
Проектирование безопасности QKDN	X.1712–X.1719
Методы обеспечения безопасности QKDN	X.1720–X.1729
БЕЗОПАСНОСТЬ ДАННЫХ	
Безопасность больших данных	X.1750–X.1759
БЕЗОПАСНОСТЬ СЕТЕЙ 5G	X.1800–X.1819

Для получения более подробной информации просьба обращаться к перечню Рекомендаций МСЭ-Т.

Рекомендация МСЭ-Т X.1254

Структура гарантии аутентификации объекта

Резюме

В Рекомендации МСЭ-Т X.1254 определяются три уровня гарантии аутентификации объекта (authentication assurance level – AAL), а также критерии и угрозы для каждого из этих трех уровней.

Кроме того:

- определяется структура управления уровнями AAL;
- на основе оценки риска приводятся руководящие указания по методам контроля, которые должны использоваться в целях смягчения угроз в отношении аутентификации;
- приводится руководство по картированию этих трех AAL в другие схемы гарантии аутентификации; и
- приводится руководство по обмену результатами аутентификации, основанными на трех AAL.

Хронологическая справка

Издание	Рекомендация	Утверждение	Исследовательская комиссия	Уникальный идентификатор*
1.0	UIT-T X.1254	07.09.2012 года	17-я	11.1002/1000/11608
2.0	UIT-T X.1254	03.09.2020 года	17-я	11.1002/1000/14260

Ключевые слова

Аутентификация, гарантия, управление определением идентичности, уровень гарантии аутентификации, уровень гарантии, AAL, IdM, LoA.

* Для получения доступа к Рекомендации наберите в адресном поле вашего браузера URL: http://handle.itu.int/, после которого укажите уникальный идентификатор Рекомендации. Например, http://handle.itu.int/11.1002/1000/11830-en.

ПРЕДИСЛОВИЕ

Международный союз электросвязи (МСЭ) является специализированным учреждением Организации Объединенных Наций в области электросвязи и информационно-коммуникационных технологий (ИКТ). Сектор стандартизации электросвязи МСЭ (МСЭ-Т) – постоянный орган МСЭ. МСЭ-Т отвечает за изучение технических, эксплуатационных и тарифных вопросов и за выпуск Рекомендаций по ним с целью стандартизации электросвязи на всемирной основе.

На Всемирной ассамблее по стандартизации электросвязи (ВАСЭ), которая проводится каждые четыре года, определяются темы для изучения исследовательскими комиссиями МСЭ-Т, которые, в свою очередь, вырабатывают Рекомендации по этим темам.

Утверждение Рекомендаций МСЭ-Т осуществляется в соответствии с процедурой, изложенной в Резолюции 1 ВАСЭ.

В некоторых областях информационных технологий, которые входят в компетенцию МСЭ-Т, необходимые стандарты разрабатываются на основе сотрудничества с ИСО и МЭК.

ПРИМЕЧАНИЕ

В настоящей Рекомендации термин "администрация" используется для краткости и обозначает как администрацию электросвязи, так и признанную эксплуатационную организацию.

Соблюдение положений данной Рекомендации осуществляется на добровольной основе. Однако данная Рекомендация может содержать некоторые обязательные положения (например, для обеспечения функциональной совместимости или возможности применения), и в таком случае соблюдение Рекомендации достигается при выполнении всех указанных положений. Для выражения требований используются слова "следует", "должен" ("shall") или некоторые другие обязывающие выражения, такие как "обязан" ("must"), а также их отрицательные формы. Употребление таких слов не означает, что от какой-либо стороны требуется соблюдение положений данной Рекомендации.

ПРАВА ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

МСЭ обращает внимание на вероятность того, что практическое применение или выполнение настоящей Рекомендации может включать использование заявленного права интеллектуальной собственности. МСЭ не занимает какую бы то ни было позицию относительно подтверждения, действительности или применимости заявленных прав интеллектуальной собственности, независимо от того, доказываются ли такие права членами МСЭ или другими сторонами, не относящимися к процессу разработки Рекомендации.

На момент утверждения настоящей Рекомендации МСЭ не получил извещение об интеллектуальной собственности, защищенной патентами, которые могут потребоваться для выполнения настоящей Рекомендации. Однако те, кто будет применять Рекомендацию, должны иметь в виду, что вышесказанное может не отражать самую последнюю информацию, и поэтому им настоятельно рекомендуется обращаться к патентной базе данных БСЭ по адресу: http://www.itu.int/ITU-T/ipr/.

СОДЕРЖАНИЕ

Введение

Цифровая идентичность – это уникальное представление объекта, участвующего в транзакции в онлайновом режиме. В основе доверия, безопасности и контроля доступа в онлайновом режиме лежит гарантия или уверенность в том, что цифровая идентичность, с которой осуществляется взаимодействие, соответствует заявленной идентичности. Определяют три типа гарантии, способствующие установлению доверия к цифровой идентичности: гарантия идентичности, гарантия аутентификации и гарантия федерации.

В настоящей Рекомендации представлена структура гарантии аутентификации. Для целей настоящей Рекомендации аутентификация определяется как процесс, посредством которого заявленная идентичность проверяется для проведения транзакции в онлайновом режиме. Для услуги, предполагающей повторные посещения, успешная аутентификация обеспечивает основанные на разумном риске гарантии того, что пользователь, обратившийся к услуге сегодня, тот же, что обращавшийся к этой услуге ранее.

Структура, определенная в этой Рекомендации, представляет поставщикам онлайновых услуг – полагающимся сторонам (RP) и поставщикам регистрационных данных (CSP) – системный подход к пониманию их рисков и определению средств контроля, помогающих снизить эти риски. Она призвана облегчить методический выбор средств контроля и стратегий снижения рисков с использованием трехэтапного процесса:

1) определение ролей и услуг для определения категорий угроз;
2) применение желаемого процесса управления рисками для определения необходимого уровня действенности средств контроля; и
3) определение технологий – протоколов, типов регистрационных данных и т. д., применимых для дальнейшего совершенствования средств контроля.

Модель на основе угроз

Настоящая Рекомендация призвана облегчить методический выбор средств контроля и стратегий снижения рисков. Предварительным шагом по обеспечению возможности выбора подходящих средств контроля и стратегий снижения рисков является определение типов рисков и угроз, связанных с ролью (ролями) и услугами поставщика онлайновых услуг. См. Рисунок 0-1.

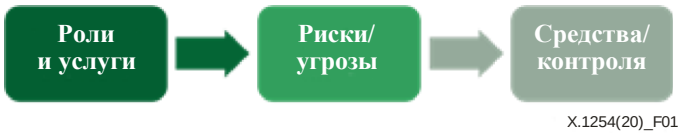

Рисунок 0-1 – Услуги, риски и средства контроля

Эта структура, организованная по категориям рисков и угроз, обеспечивает поставщикам онлайновых услуг функциональную связь между процессами оценки риска и мерами по контролю и снижению рисков.

Поставщики услуг определения идентичности могут предоставлять все, некоторые или только один из функциональных компонентов этих этапов определения цифровой идентичности. По этой причине целесообразно оценивать риски и учитывать средства контроля и подходы к снижению рисков в рамках аналогичного покомпонентного подхода к жизненному циклу цифровой транзакции. В этой Рекомендации рассматриваются риски и средства контроля на этапах управления регистрационными данными и аутентификации этого жизненного цикла. В других документах (например, [b-ISO/IEC TS 29003]) рассматриваются риски и средства контроля, относящиеся к операциям записи и проверки подлинности идентичности, а также к средствам контроля за организацией и управлением. Предполагается, что этот и другие документы будут согласованы и образуют согласованный набор базовых стандартов управления определением идентичности (как показано на Рисунке 0-2), которые при совместном использовании обеспечат процессы, меру рисков и средства контроля для жизненного цикла транзакции с использованием цифровой идентичности.

В настоящей Рекомендации также представлен каталог угроз конфиденциальности с их оценками и мерами по снижению риска, относящихся к ее сфере применения (аутентификация и управление регистрационными данными). В этой Рекомендации не рассматриваются вопросы конфиденциальности, относящиеся к проверке подлинности идентичности и регистрации идентичности.

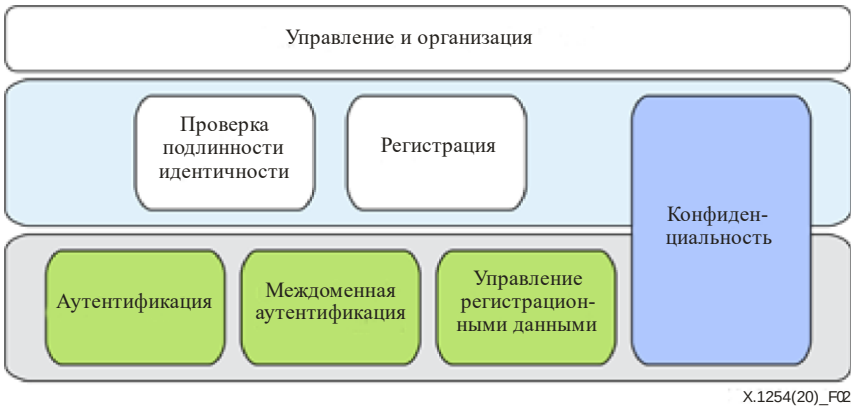

Рисунок 0-2 – Согласованные базовые стандарты управления определением идентичности

Связь с предыдущей версией настоящей Рекомендации

В первой редакции настоящей Рекомендации [b-ITU-T X.1254 (2012)] был представлен жизненный цикл транзакций с использованием цифровой идентичности, состоящий из трех этапов: регистрация и проверка подлинности идентичности, управление регистрационными данными и аутентификация объекта. С 2012 года отрасль развивалась, и появились новые концепции и подходы, такие как аутентификация без пароля и расширенная аутентификация. По этой причине отрасль ушла от концепции уровня гарантии (LoA) как единого порядка, определяющего конкретные требования к реализации. Вместо этого пользователи, сочетая надлежащее управление рисками для деловой активности и конфиденциальности с потребностями своей миссии, могут использовать уровни гарантии идентичности (IAL), уровни гарантии аутентификации (AAL) и уровни гарантии федерации (FAL) как отдельные варианты выбора. В настоящей Рекомендации основное внимание уделено уровням AAL. Уровни IAL и FAL не входят в сферу применения настоящей Рекомендации.

Рекомендация МСЭ-Т X.1254

Структура гарантии аутентификации объекта

1 Сфера применения

В настоящей Рекомендации представлена структура гарантии аутентификации объекта (entity authentication assurance – EAA) в конкретном контексте. В частности, в ней:

– устанавливаются три уровня гарантии аутентификации объекта (AAL);

– приводятся руководящие принципы для понимания этих AAL;

– определяются критерии и руководящие принципы обеспечения каждого из указанных уровней EAA;

– представлено руководство по сравнению и картированию схем гарантии аутентификации;

– представлено руководство по обмену результатами аутентификации, которые основаны на конкретных уровнях гарантии;

– представлены руководящие указания по средствам контроля, которые следует использовать в целях смягчения угроз в отношении аутентификации, основанным на оценке рисков.

2 Справочные документы

Отсутствуют.

3 Определения

3.1 Термины, определенные в других документах

В настоящей Рекомендации используются следующие термины, определенные в других документах.

3.1.1 Утверждение (assertion) [b-ITU-T X.1252] – высказывание, сделанное объектом и не сопровождаемое доказательством его истинности.

ПРИМЕЧАНИЕ. – Принято считать, что значения терминов "заявление" и "утверждение" являются весьма схожими, но несколько различаются. В настоящей Рекомендации "утверждение" является более сильным термином, чем "заявление".

3.1.2 Аутентификация (authentication) [b-ISO/IEC 18014-2] – обеспечение гарантии заявленной идентичности объекта.

3.1.3 Фактор аутентификации (authentication factor) [b-ISO/IEC 19790] – часть информации и/или процесс, используемые для аутентификации или верификации идентичности объекта.

ПРИМЕЧАНИЕ. – Факторы аутентификации подразделяются на четыре категории:

– нечто имеющееся у объекта (например, подпись устройства, паспорт, аппаратное устройство, содержащее регистрационные данные, закрытый ключ);

– нечто известное объекту (например, пароль, PIN);

– нечто, чем является объект (например, биометрические характеристики);

– нечто, что объект обычно делает (например, шаблон поведения).

3.1.4 Протокол аутентификации (authentication protocol) [b-ISO/IEC 29115] – определенная последовательность сообщений между объектом и верификатором, которая позволяет верификатору выполнить аутентификацию объекта.

3.1.5 Заявление (claim) [b-ITU-T X.1252] – высказывание того, что дело обстоит именно таким образом, без возможности представить доказательства.

ПРИМЕЧАНИЕ. – Принято считать, что значения терминов "заявление" и "утверждение" являются весьма схожими, но несколько различаются. В настоящей Рекомендации "утверждение" является более сильным термином, чем "заявление".

3.1.6 Контекст (context) [b-ITU-T X.1252] – среда с определенными граничными условиями, в которых существуют и взаимодействуют объекты.

3.1.7 Регистрационные данные (credential) [b-ITU-T X.1252] – набор данных, представляемых как доказательство заявленной идентичности и/или прав.

ПРИМЕЧАНИЕ. – Дополнительные характеристики регистрационных данных см. в Дополнении I.

3.1.8 Объект (entity) [b-ITU-T X.1252] – что-либо, что существует отдельно и обособленно и может быть определено в каком-либо контексте.

ПРИМЕЧАНИЕ. – В настоящей Рекомендации термин "объект" также используется в конкретном случае для обозначения чего-то, заявляющего свою идентичность.

3.1.9 Идентичность; частичная идентичность (identity; partial identity) [b-ISO/IEC 24760-1] – набор атрибутов, связанных с объектом.

ПРИМЕЧАНИЕ. – В конкретном контексте идентичность может содержать один или несколько идентификаторов, которые позволяют однозначно распознать объект в данном контексте.

3.1.10 Верификация информации об идентичности (identity information verification) [b-ISO/IEC 29115] – процесс проверки информации об идентичности и регистрационных данных по издателям, источникам данных или другим внутренним или внешним ресурсам в отношении аутентичности, достоверности, правильности и связи с объектом.

3.1.11 Проверка подлинности идентичности (identity proofing) [b-ISO/IEC 29115] – процесс, в рамках которого орган регистрации (RA) осуществляет сбор и верификацию информации, достаточной для идентификации объекта с определенным или предполагаемым уровнем гарантии.

3.1.12 Атака через посредника (man-in-the-middle attack) [b-ISO/IEC 29115] – атака, при которой злоумышленник может читать, вставлять или изменять сообщения, которыми обмениваются две стороны, таким образом, что сторонам это остается неизвестно.

3.1.13 Многофакторная аутентификация (multifactor authentication) [b-ISO/IEC 19790] – аутентификация с использованием по меньшей мере двух независимых факторов аутентификации.

3.1.14 Взаимная аутентификация (mutual authentication) [b-ISO/IEC 29115] – аутентификация идентичности объектов, в результате которой каждый объект убеждается в идентичности другого объекта.

3.1.15 Предотвращение отказа от участия (non-repudiation) [b-ITU-T X.1252] – способность защиты, в случае если один или несколько объектов, участвующих в каком-либо действии, не признают, полностью или частично, своего участия в этом действии.

3.1.16 Фишинг (phishing) [b-ISO/IEC 29115] – мошенничество, при котором пользователь электронной почты обманом вынуждается раскрыть личную или конфиденциальную информацию, которую мошенник затем может незаконно использовать.

3.1.17 Непризнание участия (repudiation) [b-ITU-T X.1252] – отрицание объектом, участвующим в каком-либо действии, своего участия во всем этом действии или его части.

3.1.18 Оценка риска (risk assessment) [b-ISO/IEC 27000] – общий процесс определения рисков, анализа рисков и оценки рисков.

3.1.19 Общий секрет (shared secret) [b-ISO/IEC 29115] – секрет, используемый при аутентификации и известный только объекту и верификатору.

3.1.20 Транзакция (transaction) [b-ISO/IEC 29115] – отдельное событие, происходящее между объектом и поставщиком услуг в целях достижения коммерческой или программной цели.

3.1.21 Верификация (verification) [b-ISO/IEC 29115] – процесс проверки информации путем сравнения представленной информации с ранее подтвержденной информацией.

3.1.22 Верификатор (verifier) [b-ISO/IEC 29115] – участник, который удостоверяет информацию об идентичности.

ПРИМЕЧАНИЕ. – Верификатор может участвовать в нескольких этапах структуры гарантии аутентификации объекта и осуществлять верификацию регистрационных данных и/или верификацию информации об идентичности.

3.2 Термины, определенные в настоящей Рекомендации

В настоящей Рекомендации определяются следующие термины.

3.2.1 Поставщик регистрационных данных (credential service provider) (CSP) – доверенный участник, который выпускает регистрационные данные или управляет ими.

ПРИМЕЧАНИЕ. – Это определение основано на определении, данном в [b-ISO/IEC 29115].

3.2.2 Гарантия аутентификации объекта (entity authentication assurance) (EAA) – степень уверенности, достигаемая в процессе аутентификации, в том, что объект является тем, чем, как он утверждает, является, или тем, чем, как ожидается, он является.

ПРИМЕЧАНИЕ 1. – Эта уверенность основывается на степени доверия к связи между объектом и представленной идентичностью.

ПРИМЕЧАНИЕ 2. – Это определение основывается на определении "гарантии аутентификации", данном в [b-ITU-T X.1252].

3.2.3 Идентификатор (identifier) – один или несколько атрибутов, которые уникально характеризуют объект в конкретном контексте.

ПРИМЕЧАНИЕ. – Это определение основано на определении, данном в [b-ITU-T X.1252].

3.2.4 Орган регистрации (registration authority) (RA) – доверенный участник, который устанавливает или осуществляет верификацию и гарантирует идентичность какого-либо объекта для поставщика регистрационных данных (CSP).

ПРИМЕЧАНИЕ. – Это определение основано на определении, данном в [b-ISO/IEC 29115].

3.2.5 Полагающаяся сторона (relying party) (RP) – участник, полагающийся на утверждение или заявление идентичности.

ПРИМЕЧАНИЕ. – Это определение основано на определении, данном в [b-ISO/IEC 29115].

4 Сокращения и акронимы

В настоящей Рекомендации используются следующие сокращения и акронимы.

AAL	Authentication Assurance Level	Уровень гарантии аутентификации
CSP	Credential Service Provider	Поставщик регистрационных данных
EAA	Entity Authentication Assurance	Гарантия аутентификации объекта
FAL	Federation Assurance Level	Уровень гарантии федерации
FIDO	Fast Identity On-line	Альянс Fast Identity On-line
HTML	Hypertext Markup Language	Язык разметки гипертекста
HTTP	Hypertext Transfer Protocol	Протокол передачи гипертекста
HTTPS	Hypertext Transfer Protocol Secure	Защищенный протокол передачи гипертекста
IAL	Identity Assurance Level	Уровень гарантии идентичности
IdM	Identity Management	Управление определением идентичности
IDP	Identity Provider	Поставщик данных идентичности
LoA	Level of Assurance	Уровень гарантии
MAC	Media Access Control	Управление доступом к среде передачи
MITM	Man-In-the-Middle	Атака через посредника
MITB	Man-In-the-Browser	Атака через браузер
OAuth	Open Authentication	Открытая аутентификация
OpenID	Open Identity	Открытая идентичность
OTP	One Time Password	Одноразовый пароль

PIA	Privacy Impact Assessment	Оценка воздействия на конфиденциальность
PII	Personally Identifiable Information	Информация, позволяющая установить личность
PIN	Personal Identification Number	Персональный идентификационный номер
RA	Registration Authority	Орган регистрации
RP	Relying Party	Полагающаяся сторона
SAML	Security Assertion Markup Language	Язык разметки подтверждения безопасности
TLS	Transport Layer Security	Безопасность транспортного уровня
URL	Uniform Resource Locator	Унифицированный указатель ресурса

5 Соглашения

В настоящей Рекомендации применяются следующие глагольные формы для формулировки положений:

a) "должен" обозначает требование;

b) "следует" обозначает рекомендацию;

c) "разрешается" обозначает разрешение;

d) "может" обозначает возможность или способность.

6 Последовательность процесса цифровой аутентификации

6.1 Общие положения

Цифровая идентичность – это уникальное представление объекта, участвующего в онлайновых транзакциях. Цифровая аутентификация в своей простейшей форме предполагает проверку с некоторой степенью уверенности заявленной идентичности объекта в целях предоставления ему доступа к онлайновым услугам. Зарегистрированный объект пытается пройти аутентификацию в целях получения доступа к онлайновым услугам, демонстрируя обладание аутентификатором, известным также как регистрационные данные, предоставленные ему в процессе регистрации. Онлайновая услуга, известная также как полагающаяся сторона (RP) в рамках транзакции, пытается проверить действительность аутентификатора у поставщика данных идентичности (IDP), поставщика регистрационных данных (CSP) или верификатора. Доступ к онлайновым услугам предоставляется объекту после того, как его регистрационные данные будут проверены CSP или верификатором.

Рисунок 6-1 иллюстрирует последовательность процесса цифровой аутентификации:

1) объект обращается к онлайновой услуге RP;

2) RP перенаправляет объект к CSP для аутентификации;

3) CSP проверяет наличие у объекта зарегистрированного аутентификатора(ов);

4) CSP направляет RP утверждение аутентификации, подтверждающее статус аутентификации объекта; и

5) устанавливается аутентифицированный сеанс между объектом и RP.

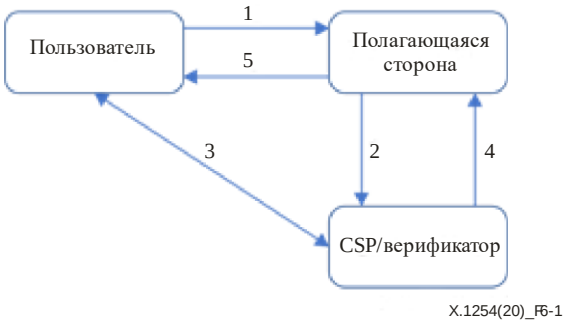

Рисунок 6-1 – Последовательность процесса цифровой аутентификации

Такое описание последовательности процесса цифровой аутентификации обеспечивает методику понимания рисков, связанных с различными ролями и функциями, вовлеченными в процесс цифровой аутентификации.

Хотя RP может иметь собственное решение для управления определением идентичности (IdM) и может сама выступать в роли CSP, в настоящей Рекомендации RP и CSP представлены как отдельные роли. Однако в любом случае функции каждой роли остаются прежними.

Кроме того, на Рисунке 6-1 роли CSP и верификатора объединены. Несмотря на то что функцию верификации обычно выполняет CSP, в некоторых случаях CSP может использовать отдельного верификатора.

Описанная последовательность процесса цифровой аутентификации предполагает, что объекты уже зарегистрированы у CSP и имеют один или несколько зарегистрированных аутентификаторов. Процессы регистрации не входят в сферу применения настоящей Рекомендации.

6.2 Гарантия цифровой идентичности

Необходимо понимать, как услуги, связанные с этапами и функциональными компонентами жизненного цикла цифровой идентичности, взаимодействуют друг с другом, обеспечивая доверие и общую уверенность в ходе онлайновой транзакции. Такое доверие обычно выражается как уровень уверенности через степени или уровни гарантии. В настоящей Рекомендации содержатся требования и руководящие указания, относящиеся к этапу гарантии аутентификации цифровой идентичности и функциям компонентов общей структуры гарантии цифровой идентичности и аутентификации. На Рисунке 6-2 приведены компоненты, описание гарантии и функциональной деятельности системы основных показателей, согласованные с документами IdM в целях обеспечения гарантии и контроля в общей структуре цифровой идентичности.

Рисунок 6-2 – Уровни гарантии цифровой идентичности

Гарантия идентичности – эта гарантия состоит из процессов, установленных для проверки связи объекта с его реальной идентичностью. Гарантия идентичности рассматривается в [b-ISO/IEC TS 29003].

Гарантия аутентификации – аутентификация устанавливает, что объект, пытающийся получить доступ к цифровой услуге, находится под контролем технологий, используемых для аутентификации. Эта гарантия состоит из процессов, используемых для проверки того, что заявленная идентичность совпадает с той, которая участвовала в процессе регистрации и ранее прошла проверку подлинности в системе.

Гарантия федерации – эта гарантия состоит из процессов, используемых для осуществления связи, защиты и утверждения идентичности, предоставляемых в разных доменах безопасности. Федерация идентичности – это обмен данными об онлайновой идентичности и аутентификационной информации между двумя или более сторонами.

Компоненты и действия гарантии идентичности, поддерживающие гарантию федерации, не входят в сферу применения данной редакции настоящей Рекомендации.

6.3 Роли

6.3.1 Общие положения

В качестве модели, ориентированной на риски, последовательность процесса цифровой аутентификации помогает определить категории угроз, связанные с тремя основными ролями – CSP, RP и объектами.

6.3.2 Поставщики онлайновых услуг

Поставщики онлайновых услуг – это организации, предлагающие онлайновые услуги, приложения и информацию с ограниченным доступом, такие как банковские услуги, медицинские услуги и услуги розничной торговли. В зависимости от способа реализации онлайновых услуг такие поставщики могут играть одну или несколько из следующих ролей:

- CSP;
- поставщик услуг определения идентичности;
- верификатор;
- RP.

6.3.3 Поставщик регистрационных данных

CSP отвечают за проверку идентификационных данных (то есть аутентификатора), представленных объектом. Процесс и степень строгости проверки определяются уровнем риска, связанного с онлайновой транзакцией, и средой, в которой будет использоваться идентичность. Функции CSP могут выполняться либо с использованием внутренней системы IdM поставщика онлайновых услуг, либо сторонней услуги определения идентичности. Кроме того, роль CSP часто отвечает за действия по управлению регистрационными данными.

6.3.4 Поставщик услуг определения идентичности

Поставщики услуг определения идентичности отвечают за проверку подлинности заявленной идентичности объекта и гарантию того, что эта заявленная идентичность связана с регистрационными данными, используемыми объектом. Процесс и степень строгости проверки определяются уровнем риска, связанного с онлайновой транзакцией, и средой, в которой будет использоваться идентичность. IDP также может отвечать за регистрацию объектов в конкретных программах и услугах. Риски и средства контроля, относящиеся к этим функциям компонента IDP, в настоящей Рекомендации не рассматриваются.

Кроме того, IDP может играть роль CSP. Поскольку эта Рекомендация посвящена управлению аутентификацией и регистрационными данными, там, где используется термин CSP, он также относится к IDP, играющему эту роль в транзакции.

6.3.5 Верификатор

Верификаторы отвечают за подтверждение идентичности объекта путем проверки находящегося в его владении и управляемого им аутентификатора(ов) с использованием протокола аутентификации. Для этого верификатору также может потребоваться проверка регистрационных данных, связывающих аутентификатор(ы) с идентификатором объекта, и их статуса. Роль верификатора часто исполняет CSP или IDP, предоставляющие регистрационные данные.

6.3.6 Полагающаяся сторона

RP принимают (полагаются на) и применяют утверждение статуса аутентификации объекта от своих собственных услуг IdM или от сторонних CSP. Чтобы принимать основанные на оценке рисков решения о том, разрешать ли конкретным объектам доступ к своим онлайновым услугам и продуктам, RP должны иметь возможность доверять информации об идентичности, получаемой от этих услуг.

6.3.7 Объекты

Для целей настоящей Рекомендации объектами считаются пользователи услуг, предлагаемых поставщиками онлайновых услуг.

Объекты несут ответственность за защиту своей идентичности и цифровых регистрационных данных от мошенничества и злоупотреблений, а также за использование своих регистрационных данных по назначению.

6.4 Компоненты процессов аутентификации

В настоящей Рекомендации представлена методика определения поставщиками услуг степени угроз и рисков, связанных с предоставляемыми ими услугами, на основе их роли (ролей), как описано в пункте 6.3, и соответствующих технологий.

Чтобы облегчить оценку конкретных рисков и угроз, связанных с онлайновой услугой, важно определить, какие функции и вспомогательные технологии участвуют в процессе аутентификации.

Процесс состоит из следующих компонентов:

- аутентификаторы – например, запоминаемые секреты (такие как пароли), устройства одноразовых паролей (OTP), смарт-карты, цифровые сертификаты и биометрические данные (такие как отпечатки пальцев);
- клиентское и серверное программное обеспечение;

- протоколы связи и аутентификации – например, язык разметки гипертекста (HTML), язык разметки подтверждения безопасности (SAML), безопасность транспортного уровня (TLS), открытая аутентификация (OAuth) и открытая идентичность (OpenID).

Транзакции аутентификации подвергаются атакам злоумышленников, нацеленным на уязвимости, связанные с одним или несколькими из перечисленных в предыдущем пункте компонентов. Соответствующие специфические угрозы и уязвимости существуют для большинства технологий аутентификации, включая аппаратное и программное обеспечение, а также протоколы передачи данных. В рамках своей деятельности по оценке рисков поставщики онлайновых услуг должны учитывать уязвимости, связанные с каждым компонентом. Конкретные категории угроз, риски и средства контроля описаны в разделе 8.

6.4.1 Аутентификаторы

Аутентификатор – это то, чем владеет и управляет объект и что он использует для аутентификации своей идентичности. С объектом может быть связано несколько аутентификаторов. То, что вы знаете, например пароль; чем вы владеете, например смарт-карта, или чем вы отличаетесь, например биометрические данные, – это факторы аутентификации. Использование одного или нескольких разных факторов повышает надежность аутентификации.

При выборе аутентификаторов, приемлемых для аутентификации в услуге, поставщик онлайновых услуг должен учитывать профиль рисков этой услуги. Кроме того, прежде чем принимать услуги CSP, RP должна изучить требования гарантии своей услуги.

Известны следующие типы аутентификаторов:

- запоминаемые секреты;
- выбираемые секреты;
- устройства, работающие по внеполосному каналу;
- однофакторные устройства OTP;
- многофакторные устройства OTP;
- однофакторные криптографические программы;
- однофакторные криптографические устройства;
- многофакторные криптографические программы;
- многофакторные криптографические устройства.

6.4.2 Аутентификатор

Структура объектов или данных, неразрывно связывающая идентичность – посредством идентификатора или идентификаторов и (возможно) дополнительных атрибутов – по крайней мере с одним аутентификатором, которым владеет и который контролирует абонент. Хотя при обычном использовании часто предполагается, что аутентификатор хранится у объекта, в настоящей Рекомендации этот термин также используется для обозначения электронных записей, хранящихся у CSP и устанавливающих связь между аутентификатором(ами) абонента и его идентичностью. Наиболее распространенной формой аутентификатора являются имя пользователя и соответствующая запись пользователя, связанная с паролем или другим аутентификатором.

7 Применение управления рисками к структуре гарантии аутентификации

7.1 Общие положения

Эффективная система IdM зависит от понимания уровней рисков, связанных с типами онлайновых услуг, предлагаемых организацией. Для понимания этих рисков поставщики онлайновых услуг должны рассмотреть свои конкретные роли в структуре, характер своих пользователей и типы данных и транзакций, обрабатываемых их приложениями.

Применение структурированной методики управления рисками даст следующие результаты: выявление рисков и угроз, решения по борьбе с ними, а также входные данные, необходимые для выбора и реализации средств контроля. В области IdM существуют специальные руководящие

принципы, помогающие организациям понять, как уровни риска соотносятся с уровнями гарантии, то есть с относительной степенью уверенности в целостности онлайновой идентичности.

Поставщики онлайновых услуг должны использовать методику управления рисками и разработать план управления рисками, связанными с цифровой аутентификацией.

Сфера охвата оценки рисков, связанных с цифровой идентичностью, должна определяться с учетом как минимум типа и уровня воздействия каждого из выявленных рисков. Также может учитываться вероятность каждого возникающего риска.

7.2 Риски, связанные с аутентификацией

При рассмотрении риска, связанного с аутентификацией, основной вопрос – что ставится под угрозу в случае ошибки, то есть каковы последствия предоставления доступа объекту, не являющемуся законным владельцем регистрационных данных и связанной с ними учетной записи.

При оценке рисков, связанных с ошибкой аутентификации, поставщики онлайновых услуг должны учитывать следующее.

- Данные. Ключевым элементом при определении того, что ставится под угрозу, является определение типов данных, обрабатываемых и защищаемых в рамках системы. Такими типами данных являются информация, позволяющая установить личность (PII), финансовая, проприетарная, общедоступная и конфиденциальная информация.
- Пользователи. Главными условиями определения и классификации конкретных рисков являются идентификация и знание пользователей системы или предприятия. Пользователи могут быть внутренними, внешними и привилегированными. Организациям следует также учитывать, связаны ли их пользователи какими-либо договорными, юридическими или иными соглашениями.
- Причины атак. Предварительно определив своих пользователей и типы данных, организация сможет лучше понимать причины атак, например если система обрабатывает и защищает информацию о банковском счете, то у злоумышленника может быть мотив для получения доступа к системе мошенническим путем для извлечения финансовой выгоды.

Поставщики онлайновых услуг должны выбирать средства контроля и другие варианты предотвращения угроз на основе оцененных рисков.

8 Категории угроз, риски и средства контроля

В этом разделе представлен каталог угроз и средств контроля, организованный по категориям угроз. Поставщикам услуг определения идентичности следует определить конкретные категории угроз, которым они подвержены, основываясь на своих ролях и услугах, связанных с аутентификацией. Средства управления сгруппированы по следующим категориям угроз:

- компрометация аутентификатора;
- компрометация транзакции;
- подмена CSP;
- подмена объекта;
- компрометация услуги аутентификации.

RP и CSP несут общую ответственность за защиту от всех угроз, связанных с аутентификацией. Роли и обязанности в рамках транзакции аутентификации должны быть четко определены и согласованы всеми сторонами.

В Таблице 8-1 представлены категории угроз аутентификации и роли, которые обычно назначаются ответственными за предотвращение этих угроз.

Таблица 8-1 – Роли и категории угроз

Роль	Категории угроз
RP	• Подмена верификатора • Компрометация транзакции • Конфиденциальность • Федерация
CSP	• Подмена верификатора • Компрометация транзакции • Подмена абонента • Компрометация аутентификатора • Компрометация услуги аутентификации • Конфиденциальность • Федерация

8.1 Уровни гарантии

В настоящей Рекомендации аутентификация – это процесс, посредством которого заявленная идентичность проверяется в целях проведения онлайновой транзакции. Повышенная строгость процессов, используемых для проверки заявленных идентичностей, повышает уверенность в том, что установленная идентичность соответствует предполагаемому субъекту этой идентичности. Гарантия аутентификации служит мерой этой уверенности, и существуют системы, или схемы, определяющие ряд относительных уровней уверенности, называемых AAL.

В настоящей Рекомендации описывается модель гарантии аутентификации, основанная на концепции выявления и предотвращения угроз и рисков для транзакций аутентификации. Во многих случаях организации, национальные органы и заинтересованные сообщества могут предпочесть создание схемы AAL, в которой сгруппированы риски, угрозы и средства контроля для среды, в которой они работают. Это дает много ощутимых преимуществ, включая установление требований для участия в транзакциях на широко определенных уровнях и возможность создания стандартных пакетов продуктов для удовлетворения потребностей сообщества.

В настоящей Рекомендации концепция уровня гарантии (LoA) как единого порядка, определяющего требования к конкретной реализации, исключается. Вместо этого пользователи могут выбирать в качестве отдельных вариантов IAL, AAL или уровень гарантии федерации (FAL), комбинируя соответствующее управление рисками для бизнеса и конфиденциальности с потребностями своей миссии. Хотя у многих систем будет одинаковый количественный уровень для каждого IAL, AAL и FAL, это не обязательное требование, и тем, кто будет применять Рекомендацию, не следует предполагать, что он будет одним и тем же в любой заданной системе.

В этих руководящих принципах описаны следующие компоненты гарантии идентичности.

- IAL – процесс проверки подлинности идентичности;
- AAL – процесс аутентификации:
- FAL – надежность утверждения в федеративной среде, используемого для передачи RP информации, связанной с аутентификацией и ее атрибутами (в соответствующих случаях).

Разделение этих категорий обеспечивает пользователям гибкость в выборе решений для гарантии идентичности и расширяет возможности для включения методов усиления защиты конфиденциальности в качестве основополагающих элементов систем идентичности на любом уровне гарантии. Например, эта модель поддерживает сценарии, допускающие взаимодействие с применением псевдонимов даже при использовании строгих многофакторных аутентификаторов.

В современной среде решение для гарантии идентичности организации не обязательно должно быть монолитом, когда все функциональные возможности обеспечиваются единственной системой или одним поставщиком. Услуги определения идентичности могут состоять из нескольких компонентов, что позволяет организациям и учреждениям использовать основанные на стандартах подключаемые решения для определения идентичности, основанные на потребностях их миссии.

Подмножества вариантов, доступных пользователю для выбора, исходя из их профилей риска и потенциального ущерба, который может причинить злоумышленник, получивший контроль над аутентификатором и доступом к системам учреждения, определяют следующие три AAL.

AAL1. AAL1 обеспечивает некоторую гарантию того, что объект контролирует аутентификатор, связанный с его учетной записью. Для AAL1 требуется однофакторная или многофакторная аутентификация с использованием широкого спектра доступных методов аутентификации. Для успешной аутентификации требуется, чтобы заявитель доказал владение аутентификатором и контроль над ним через безопасный протокол аутентификации.

AAL2. AAL2 обеспечивает высокую степень уверенности в том, что объект контролирует аутентификатор(ы), связанный(ые) с его учетной записью. Требуется доказательство права владения двумя разными факторами аутентификации и контроля над ними через безопасный протокол (протоколы) аутентификации. Для AAL2 и выше требуется использование общепринятых методов шифрования.

AAL3. AAL3 обеспечивает очень высокую степень уверенности в том, что объект контролирует аутентификатор(ы), связанный(ые) с его учетной записью. Аутентификация AAL3 основана на доказательстве владения ключом через криптографический протокол. При аутентификации AAL3 должны использоваться аппаратный криптографический аутентификатор и аутентификатор, предотвращающий подмену верификатора; оба эти требования могут выполняться одним и тем же устройством. Для аутентификации AAL3 заявители должны доказать, что они владеют двумя разными факторами аутентификации и контролируют их через безопасный(ые) протокол(ы) аутентификации. Требуются общепринятые методы шифрования.

Единый набор стандартизированных нормативных уровней гарантии в этой редакции Рекомендации не предлагается. Попытка создания единой стандартизированной структуры гарантии для всех сообществ лишит конкретные сообщества возможности управлять рисками в соответствии с их условиями. Тем не менее следует признать, что различные схемы гарантии существуют и что поставщикам услуг определения идентичности часто приходится демонстрировать соблюдение одного или нескольких наборов AAL.

Поскольку с повышением степени строгости в процессе аутентификации схемы AAL отражают все более высокие уровни уверенности при верификации заявленной идентичности, при описании средств контроля в настоящей Рекомендации вместо конкретных AAL используются относительные термины. Для тех средств контроля, которые можно изменять для повышения уверенности, условия, обеспечивающие наименьшую степень уверенности, обозначены как минимальный AAL; соответственно более высокая степень уверенность обозначена как повышенный AAL; а условия, приводящие к наибольшей степени уверенности, – как высший AAL. Таблица 8-2 дает условное представление о том, как это соотносится с некоторыми из наиболее распространенных схем гарантии аутентификации. (Обратите внимание, что приведенное в Таблице 8-2 соответствие никоим образом не предназначено для установления прямой эквивалентности между разными схемами.)

Таблица 8-2 – Уровни гарантии аутентификации

AAL	Схема из четырех AAL	Схема из трех AAL	Трехуровневая схема
Наивысший	AAL4	AAL3	Высокий
Повышенный	AAL3	AAL2	Средний
	AAL2		
Минимальный	AAL1	AAL1	Низкий

В оставшейся части этого раздела представлен расширенный набор нормативных средств контроля, сгруппированных по предотвращаемым ими угрозам. Поставщики услуг определения идентичности должны определить конкретные угрозы, которым они подвергаются, на основе своих ролей и услуг, как описано в настоящей Рекомендации. Определив их, поставщики услуг определения идентичности, чтобы получить возможность оценивать соответствие настоящей Рекомендации, должны задокументировать эти угрозы, а также соответствующие описания средств контроля и желаемые результаты, как предусмотрено в оставшейся части этого раздела.

8.2 Компрометация аутентификатора

8.2.1 Риски, связанные с компрометацией аутентификатора

Компрометация аутентификатора – это любая атака, приводящая к дублированию, подделыванию или несанкционированному раскрытию регистрационных данных, которая может использоваться для успешной аутентификации и получения несанкционированного доступа к информационной системе. Компрометация аутентификатора может произойти на любом этапе жизненного цикла IdM. Однако угрозы и средства контроля, относящиеся к сфере применения данной Рекомендации, имеют отношение только к проверке подлинности.

Регистрационные данные могут быть взломаны с помощью атак разного рода, включая фишинг, кражу, дублирование регистрационных данных, атаку повторного воспроизведения, а также атаки по методу перебора в онлайновом или автономном режиме. Предотвращение компрометации регистрационных данных не ограничивается средствами контроля для этой категории угроз. Следует отметить, что к компрометации регистрационных данных могут привести последствия отказов средств контроля для любой из категорий угроз. Например, если поставщик услуг аутентификации пострадал от утечки данных, то полученная информация может применяться для несанкционированного доступа к информационной системе.

8.2.2 Средства контроля для защиты от компрометации аутентификатора

В Таблице 8-3 приведен перечень средств контроля для защиты от компрометации аутентификатора.

Таблица 8-3 – Средства контроля для защиты от компрометации аутентификатора

Шифр	Описание средств контроля	Желаемый результат
AC-1	Для аутентификации с наивысшим AAL следует использовать аппаратный криптографический аутентификатор и аутентификатор, предотвращающий подмену верификатора; оба эти требования могут выполняться одним и тем же устройством	Для достижения желаемого AAL используются соответствующие аутентификаторы
AC-2	Для аутентификации с наивысшим AAL заявителям следует доказать, что они владеют двумя разными факторами аутентификации и контролируют их через безопасный(ые) протокол(ы) аутентификации	Для достижения желаемого AAL соблюдаются соответствующие протоколы аутентификации
AC-3	Многофакторные аутентификаторы, используемые при наивысшем AAL, следует проверять в объеме, требуемом утвержденной программой верификации криптографических модулей	Криптография аутентификатора проверяется в объеме, необходимом для достижения желаемого AAL
AC-4	Аутентификаторы, предоставляемые IDP, следует проверять на соответствие требованиям утвержденной программы верификации криптографических модулей	Используется утвержденная криптография
AC-5	Верификатору следует применять средства контроля для защиты от онлайновых атак, основанных на подборе в режиме реального времени, при использовании аутентификаторов соответствующих типов	Верификатор применяет средства контроля для защиты аутентификаторов от онлайновых атак, основанных на подборе в режиме реального времени
AC-6	Если в описании аутентификатора не указано иное, то верификатору следует ограничить количество последовательных неудачных попыток аутентификации одной учетной записи не более чем 100 попытками	Верификатор применяет средства контроля для защиты аутентификаторов от онлайновых атак, основанных на подборе в режиме реального времени

Таблица 8-3 – Средства контроля для защиты от компрометации аутентификатора

Шифр	Описание средств контроля	Желаемый результат
AC-7	Для криптографических аутентификаторов следует использовать утвержденную криптографию	Используется утвержденная криптография
AC-8	Если для аутентификации используется более одного аутентификатора, то по крайней мере один из них следует сделать устойчивым к повторению	Аутентификаторы защищены от атак повторного воспроизведения
AC-9	Все криптографические устройства для аутентификации следует сделать устойчивыми к повторению	Используются средства контроля для защиты аутентификаторов от атак повторного воспроизведения
AC-10	Соответствующие атаки по сторонним каналам следует определять методом оценки риска, выполняемой CSP	CSP выполняет надлежащие оценки рисков
AC-11	Связь между заявителем и верификатором (с использованием первичного канала в случае аутентификатора, работающего по внеполосному каналу) следует осуществлять через аутентифицированный защищенный канал	Связь между заявителем и верификатором защищена
AC-12	Однофакторные криптографические устройства, используемые при наивысшем AAL, следует проверять в объеме, требуемом утвержденной программой верификации криптографических модулей	Криптография аутентификатора проверяется в объеме, необходимом для достижения желаемого AAL
AC-13	Если в процессе аутентификации используется такое устройство, как смартфон, то разблокировку этого устройства (обычно с использованием персонального идентификационного номера (ПИН) или биометрических данных) не следует рассматривать как один из факторов аутентификации	Для достижения желаемого AAL используются соответствующие аутентификаторы
AC-14	Рекомендуется, чтобы биометрическая система допускала не более 10 последовательных неудачных попыток аутентификации. Как только этот предел достигнут, биометрический аутентификатор должен: • установить задержку не менее 30 секунд до следующей попытки, многократно увеличивая ее с каждой последующей попыткой (например, 1 минута до следующей неудачной попытки, 2 минуты до второй попытки); или • отключить биометрическую аутентификацию пользователя и предложить другой вариант (например, другой биометрический метод или PIN/пароль, если он уже не используется как обязательный фактор), если такой альтернативный метод уже доступен	Биометрическая система использует средства контроля для защиты аутентификаторов от онлайновых атак, основанных на подборе пароля

8.3 Компрометация транзакции

8.3.1 Риски, связанные с компрометацией транзакции

Компрометация транзакции – это атака, нарушающая конфиденциальность или готовность данных при их передаче между двумя сторонами. Распространенными атаками, которые могут привести

к компрометации транзакции, являются атаки через посредника (MITM), атаки через браузер (MITB), прослушивание и перехват сеансов.

8.3.2 Средства контроля для защиты от компрометации транзакций

В Таблице 8-4 приведен перечень средств контроля для защиты от компрометации транзакций.

Таблица 8-4 – Средства контроля для защиты от компрометации транзакции

Шифр	Описание средств контроля	Желаемый результат
TC-1	В ситуациях, когда верификатор и CSP являются отдельными объектами, связь между верификатором и CSP следует осуществлять через защищенный канал с взаимной аутентификацией (такой как соединение TLS, аутентифицируемое клиентом) с использованием утвержденной криптографии	Связь между верификатором и CSP защищена
TC-2	Секрет сеанса следует распределить между программным обеспечением абонента и услугой, к которой осуществляется доступ	Используются защищенные секреты сеансов
TC-3	Рекомендуется, чтобы унифицированные указатели ресурсов (URL) или контент HTTP POST [b-IETF RFC 7231] содержали идентификатор сеанса, который должен проверяться RP, чтобы гарантировать, что действия, предпринимаемые вне сеанса, не влияют на защищенный сеанс	Идентификаторы сеанса проверяются RP
TC-4	Рекомендуется, чтобы секрет предоставлялся непосредственно программным обеспечением абонента или чтобы обладание секретом доказывалось с использованием механизма шифрования	Секреты сеансов генерируются случайным образом, реализованы надлежащим способом и уничтожаются после использования
TC-5	Рекомендуется, чтобы секреты, используемые для привязки сеанса, не были доступны для незащищенных средств связи между хостом и конечной точкой абонента. После аутентификации сеансы связи не должны попадать в незащищенные каналы, например из защищенного протокола передачи гипертекста (HTTPS) в протокол передачи гипертекста (HTTP)	Передача секретов сеанса защищена
TC-6	Рекомендуется, чтобы секреты привязки сеанса генерировались хостом сеанса во время взаимодействия, обычно сразу после аутентификации пользователя	Секреты сеансов генерируются случайным образом, реализуются надлежащим способом и уничтожаются после использования
TC-7	Рекомендуется, чтобы секреты, используемые для привязки сеанса, генерировались утвержденным генератором случайных битов и содержали не менее 64 битов энтропии	Секреты сеансов генерируются случайным образом, реализуются надлежащим способом и уничтожаются после использования
TC-8	Рекомендуется, чтобы секреты, используемые для привязки сеанса, удалялись или уничтожались субъектом сеанса при выходе пользователя из системы	Секреты сеансов генерируются случайным образом, реализуются надлежащим способом и уничтожаются после использования
TC-9	Рекомендуется, чтобы секреты, используемые для привязки сеанса, отправлялись и принимались устройством с аутентифицированным защищенным каналом связи	Передача секретов сеанса защищена

Таблица 8-4 – Средства контроля для защиты от компрометации транзакции

TC-10	Рекомендуется, чтобы секреты, используемые для привязки сеанса, имели срок действия и не принимались по истечении срока, определенного CSP	Передача секретов сеанса защищена
TC-11	Рекомендуется, чтобы секреты, используемые для привязки сеанса, генерировались хостом сеанса в прямом ответе на событие аутентификации	Секреты сеансов генерируются случайным образом, реализуются надлежащим способом и уничтожаются после использования
TC-12	Cookie-файлы браузера следует помечать как доступные только в сеансах HTTPS	Передача секретов сеанса защищена
TC-13	Рекомендуется, чтобы cookie-файлы браузера были доступны для минимального реального набора имен хостов и путей	Передача секретов сеанса защищена
TC-14	Рекомендуется, чтобы непрерывность аутентифицированных сеансов основывалась на владении секретом сеанса, выдаваемым верификатором в момент аутентификации и, возможно, обновляемым во время сеанса	Секреты сеансов генерируются случайным образом, реализуются надлежащим способом и уничтожаются после использования
TC-15	Если сравнение выполняется централизованно, то всю передачу биометрических данных следует осуществлять по аутентифицированному защищенному каналу	Передача биометрической информации защищена
TC-16	Следует установить аутентифицированный защищенный канал между датчиком (или конечной точкой, содержащей незаменяемый датчик) и верификатором	Связь между верификатором и конечными точками защищена

8.4 Подмена верификатора

8.4.1 Риски, связанные с подменой верификатора

Подмена верификатора – это атака, при которой объект взаимодействует с подложным верификатором, обманным путем выведывающим у него регистрационные данные. Информация, полученная злоумышленником, может представлять значительный риск как в отношении подмены абонента, так и рассекречивания регистрационных данных. Одной из наиболее распространенных атак, связанных с подменой верификатора, является фишинг. Злоумышленник склоняет объект к передаче абонентских регистрационных данных не заслуживающему доверия клиенту, серверу или услуге и использует их для несанкционированного доступа к информационной системе.

8.4.2 Средства контроля для защиты от подмены верификатора

В Таблице 8-5 приведен список средств контроля для защиты от подмены верификатора.

Таблица 8-5 – Средства контроля для защиты от подмены верификатора

Шифр	Описание средств контроля	Желаемый результат
VI-1	Верификаторов следует проверять на соответствие требованиям утвержденной программы верификации криптографических модулей	Используется утвержденная криптография
VI-2	Следует установить аутентифицированный защищенный канал связи с верификатором посредством протокола аутентификации, устойчивого к подмене верификатора	Выходные данные аутентификатора защищены

Таблица 8-5 – Средства контроля для защиты от подмены верификатора

VI-3	Рекомендуется, чтобы аутентифицированный защищенный канал строго и необратимо связывал идентификатор канала, согласованный при создании аутентифицированного защищенного канала связи, с выходными данными аутентификатора	Выходные данные аутентификатора защищены
VI-4	Верификатору следует проверять подпись или другую информацию, используемую для доказательства стойкости к подмене верификатора	Верификаторы эффективно выполняют проверку
VI-5	В соответствующих случаях следует использовать утвержденные криптографические алгоритмы для обеспечения стойкости к подмене верификатора	Используется утвержденная криптография
VI-6	Рекомендуется, чтобы ключи, используемые для достижения стойкости к подмене верификатора, обеспечивали по крайней мере минимальную надежность защиты, указанную в соответствующем криптографическом стандарте	Подмена верификаторов невозможна
VI-7	Чтобы верификатор считался устойчивым к подмене, рекомендуется, чтобы хранящиеся у него открытые ключи были связаны с использованием утвержденных криптографических алгоритмов и обеспечивали по крайней мере минимальную надежность защиты, указанную в соответствующем криптографическом стандарте	Компрометация верификаторов невозможна
VI-8	Рекомендуется, чтобы для секретов, устойчивых к подмене верификатора, использовались утвержденные алгоритмы хеширования, а основные секреты имели по крайней мере минимальную надежность защиты, указанную в соответствующем криптографическом стандарте	Компрометация верификаторов невозможна
VI-9	Аутентификаторы, предполагающие ручной ввод выходных данных аутентификатора, такие как аутентификаторы, работающие по внеполосному каналу, и OTP-аутентификаторы, не следует считать стойкими к подмене верификатора, поскольку при ручном вводе выходные данные аутентификатора не привязаны к конкретному сеансу аутентификации	Для защиты от подмены верификатора не используются аутентификаторы, для которых требуется ручной ввод

8.5 Подмена абонента

8.5.1 Риски, связанные с подменой абонента

Подмена абонента – это атака с фальсификацией подлинности идентичности в целях нарушения процесса аутентификации и получения несанкционированного доступа к сети или информационной системе. К распространенным атакам с подменой абонента относятся спуфинг и перехват сеанса. Примером спуфинга может служить атака, при которой злоумышленник, выдавая себя за RP, подделывает адрес управления доступом к среде (MAC), принадлежащий аутентифицированному устройству, и получает несанкционированный доступ к сети. Другой пример – маскировка, когда злоумышленник, выдающий себя за легитимного пользователя, предоставляет фальсифицированные или краденые доказательства и успешно выполняет протокол сброса учетных данных.

8.5.2 Средства контроля для предотвращения подмены абонента

В Таблице 8-6 приведен список средств контроля для предотвращения подмены абонента.

Таблица 8-6 – Средства контроля для предотвращения подмены абонента

Шифр	Описание средств контроля	Желаемый результат
SI-1	Результатом процесса аутентификации является идентификатор, который следует использовать всякий раз, когда абонент аутентифицируется у данной RP	Аутентификатор(ы) привязан(ы) к соответствующему абоненту
SI-2	Рекомендуется, чтобы для удовлетворения требований данного AAL заявитель, чтобы быть признанным в качестве абонента, должен был аутентифицироваться как минимум с заданным уровнем надежности	Для достижения желаемого AAL абонент аутентифицируется с использованием соответствующего(их) аутентификатора(ов) на надлежащем уровне надежности
SI-3	Рекомендуется, чтобы при всех процессах аутентификации и повторной аутентификации по крайней мере одним аутентификатором указывалась цель аутентификации	Цель аутентификации указана
SI-4	Рекомендуется, чтобы CSP давали абоненту инструкции о том, как надлежащим образом защитить аутентификатор от кражи или потери	Абонент может восстановить аутентификатор(ы), не нарушая желаемого AAL
SI-5	Рекомендуется, чтобы аутентификация с минимальным AAL выполнялась с использованием аутентификатора любого из следующих типов: • запоминаемые секреты; • выбираемые секреты; • устройства, работающие по внеполосному каналу; • однофакторные устройства OTP; • многофакторные устройства OTP; • однофакторные криптографические программы; • однофакторные криптографические устройства; • многофакторные криптографические программы; • многофакторные криптографические устройства	Для достижения желаемого AAL абонент аутентифицируется с использованием соответствующего(их) аутентификатора(ов) на надлежащем уровне надежности
SI-6	Рекомендуется, чтобы аутентификация с повышенным AAL выполнялась с использованием многофакторного аутентификатора или комбинации двух однофакторных аутентификаторов. При использовании многофакторного аутентификатора может применяться любое из нижеследующего: • многофакторное устройство OTP; • многофакторная криптографическая программа; • многофакторное криптографическое устройство	Для достижения желаемого AAL абонент аутентифицируется с использованием соответствующего(их) аутентификатора(ов) на надлежащем уровне надежности

Таблица 8-6 – Средства контроля для предотвращения подмены абонента

SI-7	При использовании комбинации из двух однофакторных аутентификаторов в нее следует включать аутентификатор запоминаемого секрета и один располагаемый аутентификатор (нечто, чем вы владеете) из следующего списка: • выбираемый секрет; • устройство, работающее по внеполосному каналу; • однофакторное устройство OTP; • однофакторная криптографическая программа; • однофакторное криптографическое устройство	Для достижения желаемого AAL абонент аутентифицируется с использованием соответствующего(их) аутентификатора(ов) на надлежащем уровне надежности
SI-8	Рекомендуется, чтобы аутентификация с наивысшим AAL выполнялась с использованием одной из комбинаций аутентификаторов. В основе возможных комбинаций могут лежать: • многофакторное криптографическое устройство; • однофакторное криптографическое устройство в сочетании с запоминаемым секретом; • многофакторное OTP-устройство (программное или аппаратное) в сочетании с однофакторным криптографическим устройством; • многофакторное OTP- устройство (только аппаратное) в сочетании с однофакторной криптографической программой; • однофакторное OTP-устройство (только аппаратное) в сочетании с многофакторным криптографическим программным аутентификатором; • однофакторное OTP-устройство (только аппаратное) в сочетании с однофакторным криптографическим программным аутентификатором и запоминаемым секретом	Для достижения желаемого AAL абонент аутентифицируется с использованием соответствующего(их) аутентификатора(ов) на надлежащем уровне надежности
SI-9	Рекомендуется, чтобы сразу же после поступления от абонента заявления о подозрении на потерю или кражу аутентификатора CSP предоставлял механизм для отзыва или приостановки действия аутентификатора	Недействительные аутентификаторы не могут использоваться для успешной аутентификации физического лица
SI-10	Рекомендуется, чтобы CSP предоставил абоненту способ доказательства CSP его подлинности с помощью резервного или альтернативного аутентификатора для безопасного сообщения о потере, краже или повреждении аутентификатора. Этот резервный аутентификатор должен быть запоминаемым секретом или физическим аутентификатором	Абонент может восстановить аутентификатор(ы), не нарушая желаемого AAL

Таблица 8-6 – Средства контроля для предотвращения подмены абонента

SI-11	Рекомендуется, чтобы приостановка действия была обратимой, если абонент успешно докажет CSP свою подлинность с помощью действительного (не приостановленного) аутентификатора и запросит повторную активацию аутентификатора, действие которого приостановлено таким образом	Абонент может восстановить аутентификатор(ы), не нарушая желаемого AAL
SI-12	Рекомендуется, чтобы по истечении срока действия аутентификатора он больше не использовался для аутентификации	Недействительные аутентификаторы не могут использоваться для успешной аутентификации физического лица
SI-13	CSP следует требовать от абонентов сдачи или уничтожения любых физических аутентификаторов, содержащих сертификаты атрибутов, подписанные CSP, как только это станет практически возможным, после того как аутентификатор станет недействительным по причине истечения срока действия, аннулирования, прекращения действия, обновления или по другим причинам, определенным CSP	Недействительные аутентификаторы не могут использоваться для успешной аутентификации физического лица
SI-14	CSP следует немедленно аннулировать привязку аутентификаторов, как только перестает существовать онлайновая идентичность, по запросу абонента или если CSP установит, что абонент больше не отвечает его требованиям	Недействительные аутентификаторы не могут использоваться для успешной аутентификации физического лица
SI-15	Биометрические данные следует использовать только в составе многофакторной аутентификации с физическим аутентификатором (чем-то, что у вас имеется)	Биометрические данные используются надлежащим образом в качестве аутентификаторов
SI-16	При повышенном AAL CSP в дополнение к запоминаемому секрету или одному или нескольким биометрическим параметрам следует привязать к онлайновой идентичности абонента хотя бы один, а лучше два или более физических аутентификаторов (нечто, что у вас имеется)	Аутентификатор(ы) привязан(ы) к соответствующему абоненту
SI-17	При повышенном AAL, если регистрация и привязка не могут быть завершены в процессе одной физической встречи или электронной транзакции, следует использовать следующие методы гарантии того, что на протяжении всех процессов в качестве заявителя выступает одна и та же сторона. При удаленных транзакциях 1. Рекомендуется, чтобы заявители идентифицировали себя при каждой новой транзакции, предоставляя временный секрет либо секрет, созданный во время предыдущей транзакции, либо отправленный по номеру телефона заявителя, адресу электронной почты или почтовому адресу из учетной записи. 2. Секреты долгосрочных аутентификаторов следует выдавать заявителю только в ходе защищенных сеансов.	Аутентификатор(ы) привязан(ы) к соответствующему абоненту

Таблица 8-6 – Средства контроля для предотвращения подмены абонента

	При транзакциях с личным присутствием 1. Рекомендуется, чтобы заявители идентифицировали себя лично, используя либо секрет, как описано для удаленной транзакции в пункте 1 предыдущего пункта, либо биометрические данные, записанные во время предыдущей встречи. 2. Не следует повторно использовать временные секреты. 3. Если во время физической транзакции CSP выдает долгосрочные секреты-аутентификаторы, то их следует загружать локально в физическое устройство, выданное заявителю лично или доставленное по адресу из учетной записи	
SI-18	При привязывании к учетной записи абонента дополнительного аутентификатора CSP следует сначала потребовать от абонента аутентифицировать себя по крайней мере с тем AAL, на котором будет использоваться новый аутентификатор	Аутентификатор(ы) привязан(ы) к соответствующему абоненту
SI-19	При повышенном AAL, если абонент утратил все аутентификаторы, относящиеся к фактору, необходимому для выполнения многофакторной аутентификации, этот абонент должен повторить процесс проверки подлинности идентичности	Абонент может восстановить аутентификатор(ы), не нарушая требуемого AAL
SI-20	При повышенном AAL в случае замены утраченного фактора аутентификации CSP следует потребовать от заявителя аутентификации с использованием аутентификатора любого оставшегося фактора для подтверждения привязки к существующей идентичности	Абонент может восстановить аутентификатор(ы), не нарушая требуемого AAL
SI-21	Для подтверждения продолжения участия абонента в аутентифицированном сеансе следует выполнять периодическую повторную аутентификацию сеансов	Абонент должен периодически повторять аутентификацию с надлежащим(и) аутентификатором(ами) с надежностью, достаточной для достижения желаемого AAL
SI-22	Следует периодически выполнять повторную аутентификацию сеансов абонента. a) При минимальном AAL повторную аутентификацию абонента во время продленного сеанса следует повторять независимо от активности пользователя, по крайней мере каждые 30 дней. b) При минимальном AAL по истечении этого срока сеанс следует завершать (зарегистрировать выход). c) При повышенном AAL повторную аутентификацию абонента во время продленного сеанса следует повторять независимо от активности пользователя, по крайней мере каждые 12 часов.	Абонент должен периодически повторять аутентификацию с надлежащим(и) аутентификатором(ами) с надежностью, достаточной для достижения желаемого AAL

Таблица 8-6 – Средства контроля для предотвращения подмены абонента

	d) При повышенном AAL повторную аутентификацию абонента следует повторять после любого периода бездействия, продолжавшегося 30 минут или дольше. e) При повышенном AAL по истечении любого из этих сроков сеанс следует завершать (зарегистрировать выход). f) При наивысшем AAL аутентификацию абонента во время продленного сеанса следует повторять, независимо от активности пользователя, по крайней мере каждые 12 часов. g) При наивысшем AAL повторную аутентификацию абонента следует повторять после любого периода бездействия, продолжавшегося 15 минут или дольше. h) При наивысшем AAL по истечении любого из сроков (f) или (g) сеанс следует завершать (зарегистрировать выход). i) При наивысшем AAL периодическую повторную аутентификацию сеансов абонента следует выполнять с использованием всех первоначальных факторов аутентификации	
SI-23	Сеанс не следует продлевать только на основе представления секрета сеанса	Абонент должен периодически повторять аутентификацию с надлежащим(и) аутентификатором(ами) с надежностью, достаточной для достижения желаемого AAL
SI-24	Если сеанс был завершен по тайм-ауту или в силу другого действия, следует потребовать, чтобы пользователь установил новый сеанс путем повторной аутентификации	Абонент должен периодически повторять аутентификацию с надлежащим(и) аутентификатором(ами) с надежностью, достаточной для достижения желаемого AAL
SI-25	Рекомендуется, чтобы секреты сеанса были непостоянными. То есть они не должны сохраняться при перезапуске связанного с ними приложения или перезагрузке хоста	Абонент должен периодически повторять аутентификацию с надлежащим(и) аутентификатором(ами) с надежностью, достаточной для достижения желаемого AAL

8.6 Компрометация услуги аутентификации, связанные с ней риски и средства контроля

8.6.1 Риски, связанные с компрометацией услуги аутентификации

Компрометация услуги аутентификации – это атака на объект, предоставляющий услуги определения идентичности, которая делает его неработоспособным, неточным, недоступным или неспособным функционировать надлежащим образом. Услугу аутентификации может скомпрометировать любой изъян в среде управления информационной системой объекта, который можно использовать. Например, злоумышленник может использовать неисправленную уязвимость программного обеспечения и получить несанкционированный привилегированный доступ к информационной системе услуги аутентификации.

8.6.2 Средства контроля для предотвращения компрометации услуги аутентификации

В Таблице 8-7 приведен перечень средств контроля для предотвращения компрометации услуги аутентификации.

Таблица 8-7 – Средства контроля для предотвращения компрометации услуги аутентификации

Шифр	Описание средств контроля	Желаемый результат
ASC-1	CSP следует использовать средства безопасности, ориентированные на заданный уровень безопасности, как указано в [b-ISO/IEC 27002] или эквивалентном стандарте	Целостность услуги аутентификации защищена от взлома
ASC-2	CSP следует обеспечить соблюдение минимальных мер контроля, связанных с гарантией безопасности, с учетом контекста общесистемного риска	Целостность услуги аутентификации защищена от взлома
ASC-3	Если сравнение выполняется централизованно, следует производить отзыв биометрических данных, что в [b-ISO/IEC 24745] называется защитой биометрических шаблонов	Услуга аутентификации защищает биометрическую информацию
ASC-4	Рекомендуется, чтобы цель аутентификации определялась самим аутентификатором, хотя многофакторные криптографические устройства могут устанавливать цель путем повторного ввода другого фактора аутентификации в конечной точке, в которой используется аутентификатор	Целевой объект аутентификации устанавливается только аутентификатором
ASC-5	В течение всего жизненного цикла цифровой идентичности CSP следует вести учет всех аутентификаторов, которые связаны или были связаны с каждой идентичностью	Информация об аутентификаторах регистрируется и сохраняется
ASC-6	CSP или верификатору также следует хранить информацию, необходимую для регулирования попыток аутентификации, когда это необходимо	Информация об аутентификаторах регистрируется и сохраняется
ASC-7	Записи, создаваемые CSP, должны содержать дату и время привязки аутентификатора к учетной записи	Информация об аутентификаторах регистрируется и сохраняется
ASC-8	Аутентификаторы следует привязывать к учетным записям абонентов одним из следующих способов: • выдача CSP в ходе регистрации; или • связь с приемлемым для CSP аутентификатором, предоставленным абонентом	Аутентификаторы надлежащим образом привязаны к учетным записям абонента
ASC-9	Когда к учетной записи абонента привязывается новый аутентификатор, CSP следует убедиться, что протокол привязки и протокол для предоставления связанного(ых) с ним ключа (ключей) выполнены на уровне безопасности, соразмерном с AAL, на котором будет использоваться аутентификатор	Аутентификаторы надлежащим образом привязаны к учетным записям абонента
ASC-10	При привязке многофакторных аутентификаторов для связи с аутентификатором следует требовать многофакторной аутентификации или связи с сеансом, в котором только что была выполнена проверка подлинности идентичности	Аутентификаторы надлежащим образом привязаны к учетным записям абонента

8.7 Конфиденциальность, риски и средства контроля

8.7.1 Риски для защиты конфиденциальности

Цифровая аутентификация поддерживает защиту конфиденциальности, уменьшая риски несанкционированного доступа к информации частных лиц. В то же время, поскольку проверка подлинности идентичности, аутентификация, авторизация и федерация связаны с обработкой

индивидуальной информации, эти функции также могут создавать риски для защиты конфиденциальности. Таким образом данные руководящие принципы включают в себя требования и соображения, относящиеся к конфиденциальности, которые помогут снизить потенциальные риски для защиты конфиденциальности.

CSP должен провести оценку рисков для защиты конфиденциальности, относящихся к хранению записей. В оценку рисков для защиты конфиденциальности могут входить:

1) вероятность того, что хранение записи приведет к проблемам для абонента, таким как навязчивость или несанкционированный доступ к информации;

2) последствия в случае возникновения такой проблемы.

Рекомендуется, чтобы CSP были в состоянии рационально обосновать любые ответные меры, которые они принимают в отношении выявленных рисков для защиты конфиденциальности, включая принятие риска, снижение риска и распределение риска. Получение согласия абонента является формой распределения риска и, следовательно, подходит только тогда, когда можно обоснованно ожидать, что у абонента имеется возможность оценить и принять свою часть риска.

8.7.2 Средства контроля конфиденциальности

В Таблице 8-8 приведен список средств контроля конфиденциальности.

Таблица 8-8 – Средства контроля конфиденциальности

Шифр	Описание средств контроля	Желаемый результат
P-1	Когда для получения онлайнового доступа предоставляется самозаявленная PII или другая личная информация, IDP следует выбрать как минимум подходящий AAL	CSP обеспечивает соблюдение политики конфиденциальности и средства контроля конфиденциальности в отношении аутентификации
P-2	CSP следует соблюдать надлежащую собственную политику хранения записей в соответствии с применимыми законами, правилами и нормами. Если CSP решает хранить записи в отсутствие каких-либо обязательных требований, CSP следует провести процесс управления рисками, включая оценку рисков для конфиденциальности и безопасности, чтобы определить, как долго следует хранить записи и следует ли проинформировать абонента об этой политике хранения	CSP аутентифицирует абонентов в соответствии с применимыми законами, правилами и нормами
P-3	Следует позаботиться о том, чтобы использование PII ограничивалось первоначальной целью ее сбора	CSP собирает минимальное количество PII для достижения желаемого AAL
P-4	Если использование PII не связано с аутентификацией или соблюдением закона или судебного предписания, то CSP следует уведомить абонента и получить его согласие	CSP аутентифицирует абонентов в соответствии с применимыми законами, правилами и нормами
P-5	IDP следует провести или опубликовать оценку воздействия на конфиденциальность (PIA), охватывающую сбор PII и другой личной информации, в соответствии с применимыми законами и правилами	CSP проводит PIA

Таблица 8-8 – Средства контроля конфиденциальности

P-6	CSP не следует использовать или разглашать информацию об абонентах ни для каких целей, кроме аутентификации, снижения риска мошенничества или соблюдения закона или судебного предписания, если только CSP не направит абоненту четкое уведомление и не получит согласие на ее использование в других целях	CSP аутентифицирует абонентов в соответствии с применимыми законами, правилами и нормами
P-7	CSP следует использовать соответствующим образом настроенные средства защиты конфиденциальности, определенные в [ISO/IEC 27002] или эквивалентном стандарте	CSP обеспечивает соблюдение политики конфиденциальности и средства контроля конфиденциальности в отношении аутентификации
P-8	CSP не следует делать согласие условием обслуживания	CSP аутентифицирует абонентов в соответствии с применимыми законами, правилами и нормами
P-9	CSP может связать аутентификатор пониженного AAL с идентичностью повышенного AAL, но если абонент аутентифицирован на пониженном AAL, то CSP не следует раскрывать ему личную информацию, даже если она самозаявлена	CSP собирает минимальное количество PII или личной информации для достижения желаемого AAL
P-10	Согласие абонента на использование информации в дополнительных целях не следует делать условием предоставления услуг аутентификации	CSP аутентифицирует абонентов в соответствии с применимыми законами, правилами и нормами

Дополнение I

Пример строгой аутентификации с использованием Рекомендации [b-ITU-T X.1278]

(Данное Дополнение не является неотъемлемой частью настоящей Рекомендации)

I.1 Введение

В Рекомендациях "Структура универсальной аутентификации" [b-ITU-T X.1277] и "Протокол клиент-аутентификатор/универсальная двухфакторная схема" [b-ITU-T X.1278] предлагаются подходы к аутентификации и гарантии аутентификации, обеспечивающие строгую аутентификацию на основе открытых совместимых Рекомендаций. В этом Дополнении представлен пример строгой аутентификации с использованием [b-ITU-T X.1278].

I.2 Категории угроз

На Рисунке I.1 показаны угрозы, сгруппированные по двум категориям.

1) Масштабируемые атаки – количество целей, будь то 1000 или 1 000 000, не влияет на стоимость атаки:
   a) удаленные атаки на серверы и кража паролей. Эта атака очень опасна, так как пользователи не могут от нее защититься – это должны делать RP. Однако пользователи могут усугубить ситуацию: если они сообщают одни и те же пароли нескольким RP, то взлом наименее защищенной RP повлияет на все остальные;
   b) удаленные атаки на множество пользовательских устройств. Например, попытка похитить данные с устройства в целях подмены пользователя;
   c) удаленные атаки также могут привести к злоупотреблению данными на пользовательских устройствах в целях подмены пользователя;
   d) удаленные атаки на множество пользовательских устройств в целях взлома сеанса со строгой аутентификацией. Это называется атакой MITB.

Интересно отметить, что одни лишь смарт-карты не защищают от злоупотребления регистрационными данными, поскольку смарт-карта не различает, введен ли ПИН-код самим пользователем или какой-нибудь вредоносной программой, похитившей его у пользователя.

2) Физические атаки – когда требуется физический доступ к устройству. Физические атаки не масштабируются, поскольку кража (активных) смартфонов сопряжена со значительными затратами на каждое устройство:
   a) физические атаки на пользовательские устройства для кражи данных в целях подмены;
   b) физические атаки на пользовательские устройства для злоупотребления ими в целях подмены.

I.3 Рекомендация [b-ITU-T X.1278] обеспечивает возможность "высоконадежной строгой аутентификации"

Высоконадежная строгая аутентификация означает:

1) использование двух или более факторов;
2) по крайней мере один из факторов применяет криптографию с открытым ключом;
3) отсутствие подверженности фишингу, MITM и другим атакам, нацеленным на регистрационные данные.

Основные отличительные особенности подхода быстрой идентификации онлайн (FIDO):

- отсутствие общих секретов – используется то, что у вас имеется (например, аппаратные устройства), и то, чем вы отличаетесь (например, отпечатки пальцев);
- вместо симметричных общих секретов используется криптография с открытым ключом;

- пользователь проверяется по аутентификатору, а затем RP аутентифицирует этот аутентификатор; и
- стойкая к фишингу многофакторная аутентификация.

Эти подходы соответствуют следующим принципам безопасности и конфиденциальности:

- услуги и учетные записи не связаны друг с другом;
- в протоколе отсутствует третья сторона;
- биометрические данные, если они используются, никогда не покидают устройство;
- криптографические ключи остаются в устройстве;
- на стороне сервера общие секреты отсутствуют; и
- основа криптографии с открытым ключом.

X.1254(20)_FI.1

Рисунок I.1 – Классификация угроз

I.4 Старая система аутентификации на основе паролей

Типичным процессам аутентификации на основе паролей присущ ряд рисков, как показано на Рисунке I.2:

1) пароли могут быть похищены с сервера (утечка данных);
2) пароли могут вводиться в ненадежных приложениях или на ненадежных веб-сайтах (фишинг);
3) слишком большое количество паролей, которые нужно помнить, приводит к их повторному использованию (становится проще угадывать пароли между веб-сайтами);
4) неудобно вводить пароли на телефонах (пользователи выбирают пароли, которые легко угадать).

Рисунок I.2 – Старая система аутентификации на основе паролей

I.5 Новая система аутентификации на основе Рекомендации [b-ITU-T X.1278]

FIDO отделяет аспект аутентификации от аспекта идентичности. На Рисунке I.3 показаны преимущества этого подхода:

1) секреты не хранятся на сервере (защита от утечки данных);

2) аутентификаторы невозможно обманом выведать с помощью фишинга;

3) не нужно запоминать пароли и в процессе аутентификации не требуется никаких дополнительных усилий;

4) удобство одного жеста для пользователя.

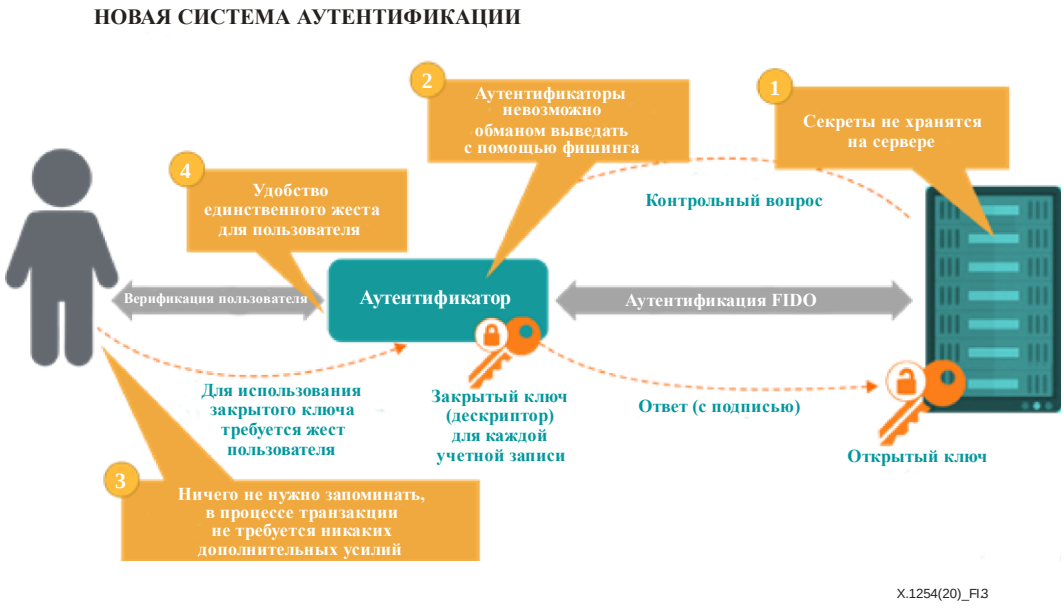

Рисунок I.3 – Новая система аутентификации на основе Рекомендации [b-ITU-T X.1278]

I.6 Совместимость и сертификация

Помимо создания новых методов аутентификации повышается надежность решений аутентификации за счет совместимости и сертификационных испытаний:

- повышенная приемлемость строгой аутентификации для пользователей или потребителей;

- снижение риска и воздействия кражи идентичности благодаря более широкому распространению строгой аутентификации;
- повышение удобства для пользователей благодаря широкому спектру устройств и услуг аутентификации;
- сокращение расходов повышает применение строгой аутентификации.

Библиография

[b-ITU-T X.1252]	Рекомендация МСЭ-Т X.1252 (2010 год), *Базовые термины и определения в области управления определением идентичности*
[b-ITU-T X.1254 (2012)]	Рекомендация МСЭ-Т X.1254 (2012 год), *Структура гарантии аутентификации объекта*
[b-ITU-T X.1277]	Recommendation ITU-T X.1277 (2018), *Universal authentication framework*
[b-ITU-T X.1278]	Recommendation ITU-T X.1278 (2018), *Client to authenticator protocol/Universal 2-factor framework*
[b-ISO/IEC 18014-2]	ISO/IEC 18014-2:2009, *Information technology – Security techniques – Time-stamping services – Part 2: Mechanisms producing independent tokens*
[b-ISO/IEC 19790]	ISO/IEC 19790:2012, *Information technology – Security techniques – Security requirements for cryptographic modules*
[b-ISO/IEC 24745]	ISO/IEC 24745:2011, *Information technology – Security techniques – Biometric information protection*
[b-ISO/IEC 24760-1]	ISO/IEC 24760-1:2019, *IT security and privacy – A framework for identity management – Part 1: Terminology and concepts*
[b-ISO/IEC 27000]	ISO/IEC 27000 (2018), *Information technology – Security techniques – Information security management systems – Overview and vocabulary*
[b-ISO/IEC 27002]	ISO/IEC 27002:2013, *Information technology – Security techniques – Code of practice for information security controls*
[b-ISO/IEC TS 29003]	Technical Specification ISO/IEC TS 29003:2018, *Information technology – Security techniques – Identity proofing*
[b-ISO/IEC 29115]	ISO/IEC 29115:2013, *Information technology – Security techniques – Entity authentication assurance framework*
[b-IETF RFC 7231]	IETF RFC 7231 (2014), *Hypertext transfer protocol (HTTP/1.1): Semantics and content*

СЕРИИ РЕКОМЕНДАЦИЙ МСЭ-Т

Серия A	Организация работы МСЭ-Т
Серия D	Принципы тарификации и учета и экономические и стратегические вопросы международной электросвязи/ИКТ
Серия E	Общая эксплуатация сети, телефонная служба, функционирование служб и человеческие факторы
Серия F	Нетелефонные службы электросвязи
Серия G	Системы и среда передачи, цифровые системы и сети
Серия H	Аудиовизуальные и мультимедийные системы
Серия I	Цифровая сеть с интеграцией служб
Серия J	Кабельные сети и передача сигналов телевизионных и звуковых программ и других мультимедийных сигналов
Серия K	Защита от помех
Серия L	Окружающая среда и ИКТ, изменение климата, электронные отходы, энергоэффективность; конструкция, прокладка и защита кабелей и других элементов линейно-кабельных сооружений
Серия M	Управление электросвязью, включая СУЭ и техническое обслуживание сетей
Серия N	Техническое обслуживание: международные каналы передачи звуковых и телевизионных программ
Серия O	Требования к измерительной аппаратуре
Серия P	Качество телефонной передачи, телефонные установки, сети местных линий
Серия Q	Коммутация и сигнализация, а также соответствующие измерения и испытания
Серия R	Телеграфная передача
Серия S	Оконечное оборудование для телеграфных служб
Серия T	Оконечное оборудование для телематических служб
Серия U	Телеграфная коммутация
Серия V	Передача данных по телефонной сети
Серия X	**Сети передачи данных, взаимосвязь открытых систем и безопасность**
Серия Y	Глобальная информационная инфраструктура, аспекты межсетевого протокола, сети последующих поколений, интернет вещей и "умные" города
Серия Z	Языки и общие аспекты программного обеспечения для систем электросвязи

Отпечатано в Швейцарии
Женева, 2021 г.