ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 70262.2— 2025

Защита информации

ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ

Уровни доверия аутентификации

Издание официальное

Москва
Российский институт стандартизации
2025

gost.e-ecolog.ru

Предисловие

1 РАЗРАБОТАН Федеральной службой по техническому и экспортному контролю (ФСТЭК России), Федеральным автономным учреждением «Государственный научно-исследовательский испытательный институт проблем технической защиты информации Федеральной службы по техническому и экспортному контролю» (ФАУ «ГНИИИ ПТЗИ ФСТЭК России») и Акционерным обществом «Аладдин Р.Д.» (АО «Аладдин Р.Д.»)

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 362 «Защита информации»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 29 мая 2025 г. № 503-ст

4 ВВЕДЕН ВПЕРВЫЕ

*Правила применения настоящего стандарта установлены в статье 26 Федерального закона от 29 июня 2015 г. № 162-ФЗ «О стандартизации в Российской Федерации». Информация об изменениях к настоящему стандарту публикуется в ежегодном (по состоянию на 1 января текущего года) информационном указателе «Национальные стандарты», а официальный текст изменений и поправок — в ежемесячном информационном указателе «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ближайшем выпуске ежемесячного информационного указателя «Национальные стандарты». Соответствующая информация, уведомление и тексты размещаются также в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет (*gost.e-ecolog.ru

© Оформление. ФГБУ «Институт стандартизации», 2025

Настоящий стандарт не может быть полностью или частично воспроизведен, тиражирован и распространен в качестве официального издания без разрешения Федерального агентства по техническому регулированию и метрологии

Содержание

1 Область применения 1
2 Нормативные ссылки 1
3 Термины и определения 2
4 Общие положения 9
5 Виды и средства аутентификации 13
6 Уровни доверия аутентификации 17
Приложение А (справочное) Общая характеристика уровней доверия аутентификации 19
Библиография 21

Введение

Одной из главных задач защиты информации при ее автоматизированной (автоматической) обработке является управление доступом. Решение о предоставлении доступа для использования информационных и вычислительных ресурсов средств вычислительной техники, а также ресурсов автоматизированных (информационных) систем основывается на результатах идентификации и аутентификации.

Физическое лицо при использовании информационных и вычислительных ресурсов средств вычислительной техники, как правило, выполняет операции по обработке данных через вычислительные процессы. Аналогично осуществляется обработка информации и при использовании ресурсов автоматизированных (информационных) систем другими («внешними») автоматизированными (информационными) системами или средствами вычислительной техники. Это порождает риски неоднозначного сопоставления конкретного вычислительного процесса определенному физическому лицу и/или конкретному «внешнему» ресурсу средств вычислительной техники. Устанавливая для пользователей правила управления доступом к защищаемой информации и сервисам, обеспечивающим ее обработку, необходимо учитывать не только ее конфиденциальность, но и указанные риски. Основой для их снижения является установление точного соответствия как между физическим лицом (ресурсом) и вычислительными процессами, которыми оно представлено при выполнении операций, так и между вычислительными процессами и ресурсами средств вычислительной техники, которые выполняют данные операции. Данное соответствие, как правило, устанавливается при регистрации ресурса как объекта или субъекта доступа и физического лица как пользователя (субъекта доступа), проверяется при опознавании субъекта доступа (ресурса или физического лица) по предъявленному идентификатору доступа, подтверждается при проверке его подлинности и обеспечивает определенную уверенность в том, что обработка данных вычислительными процессами действительно инициирована физическим лицом или ресурсом, имеющим на это право.

При разработке настоящего стандарта учитывались нормы, определенные ГОСТ Р 58833, а также правила аутентификации, рекомендованные ГОСТ Р 59383 с учетом [1], [2], [3].

Для понимания положений настоящего стандарта необходимы знания основ информационных технологий и методов (способов) защиты информации.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Защита информации

ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ

Уровни доверия аутентификации

Information protection. Identification and authentication.
Authentication assurance levels

Дата введения — 2025—10—01

1 Область применения

Настоящий стандарт устанавливает единообразную организацию процесса аутентификации субъектов и объектов доступа в средствах защиты информации, в том числе реализующих криптографическую защиту, средствах вычислительной техники и автоматизированных (информационных) системах, а также определяет общие правила аутентификации, которые обеспечивают необходимую уверенность в ее результатах.

Положения настоящего стандарта не исключают применение криптографических и биометрических методов (алгоритмов) при аутентификации, но не устанавливают требования по их реализации.

Настоящий стандарт определяет основное содержание процесса аутентификации, состав участников, их ролей и действий при аутентификации, которые рекомендуются к реализации при разработке, внедрении и совершенствовании правил, механизмов и технологий управления доступом. Стандарт устанавливает уровни доверия аутентификации, а также виды аутентификации и перечень средств аутентификации, необходимых к применению на каждом из уровней доверия.

Положения настоящего стандарта могут использоваться при управлении доступом к информационным ресурсам, вычислительным ресурсам средств вычислительной техники, ресурсам автоматизированных (информационных) систем, средствам вычислительной техники и автоматизированным (информационным) системам в целом.

Положения настоящего стандарта применяются совместно с документами по стандартизации, регламентирующими вопросы идентификации.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

ГОСТ Р 50922 Защита информации. Основные термины и определения

ГОСТ Р 58833—2020 Защита информации. Идентификация и аутентификация. Общие положения

ГОСТ Р 59383 Информационные технологии. Методы и средства обеспечения безопасности. Основы управления доступом

ГОСТ Р 70262.1 Защита информации. Идентификация и аутентификация. Уровни доверия идентификации

ГОСТ Р 70916 Блоки сложно-функциональные. Термины и определения

ГОСТ Р ИСО/МЭК 27005 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности

Примечание — При пользовании настоящим стандартом целесообразно проверить действие ссылочных стандартов в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет или по ежегодному информационному указа-

Издание официальное

телю «Национальные стандарты», который опубликован по состоянию на 1 января текущего года, и по выпускам ежемесячного информационного указателя «Национальные стандарты» за текущий год. Если заменен ссылочный стандарт, на который дана недатированная ссылка, то рекомендуется использовать действующую версию этого стандарта с учетом всех внесенных в данную версию изменений. Если заменен ссылочный стандарт, на который дана датированная ссылка, то рекомендуется использовать версию этого стандарта с указанным выше годом утверждения (принятия). Если после утверждения настоящего стандарта в ссылочный стандарт, на который дана датированная ссылка, внесено изменение, затрагивающее положение, на которое дана ссылка, то это положение рекомендуется применять без учета данного изменения. Если ссылочный стандарт отменен без замены, то положение, в котором дана ссылка на него, рекомендуется применять в части, не затрагивающей эту ссылку.

3 Термины и определения

В настоящем стандарте применены термины по ГОСТ Р 50922, ГОСТ Р 70916, а также следующие термины с соответствующими определениями:

3.1

аутентификационная информация: Информация, используемая для аутентификации субъекта доступа или объекта доступа.

[Адаптировано из ГОСТ Р 58833—2020, пункт 3.3]

3.2 **аутентификатор:** Аутентификационная информация [и другая информация (данные), необходимая при аутентификации] и устройство аутентификации (при записи аутентификационной информации в устройство аутентификации), ассоциированные с субъектом (объектом) доступа, которые назначаются при регистрации и используются при аутентификации субъекта (объекта) доступа.

Примечания

1 Аутентификатор может представлять собой: в простейшем случае — запоминаемый секрет (например, пароль); в других случаях — совокупность устройства аутентификации, которым владеет субъект доступа, и, например, записанного в него электронного удостоверения.

2 К другой информации (данным), необходимой при аутентификации, может относиться, например, информация, позволяющая получить доступ к информации в устройстве аутентификации (например, PIN-код или биометрические персональные данные), или информация, используемая при восстановлении или подтверждении аутентификационной информации, или информация, используемая для организации аутентификационного обмена (например, криптографические ключи, уникальный идентификатор субъекта доступа и т. п.).

3 При аутентификации аутентификаторы используются вместе (в составе) со средствами аутентификации.

4 Кроме аутентификационной и другой информации (данных), необходимой при аутентификации, в устройство аутентификации может помещаться и идентификационная информация или совокупность идентификационной, аутентификационной и другой информации в виде электронного удостоверения[1)].

3.3 **аутентификационный обмен:** Последовательность одной или нескольких передач сообщений, содержащих аутентификационную и (или) другую информацию, необходимую при аутентификации, которые выполняются в рамках протокола аутентификации.

3.4 **аутентификационный секрет (секрет):** Аутентификатор, который необходимо хранить в тайне.

Примечания

1 Не все аутентификаторы могут считаться аутентификационными секретами, так как некоторые из них нельзя сохранить в тайне. Например, биометрические персональные данные, характеризующие биологические особенности человека, которые невозможно сохранить в тайне (отпечаток пальца, геометрические характеристики лица и т. п.). Биометрические персональные данные могут использоваться при аутентификации, но не могут считаться аутентификационными секретами. При этом не исключается необходимость выполнения мероприятий по их защите.

2 Некоторые секреты, например криптографические ключи, используются при аутентификации, но при этом они могут не являться аутентификаторами.

3 Аутентификационные секреты могут быть долгосрочными и краткосрочными. К долгосрочным секретам относятся те, которые действуют продолжительное время и, как правило, значение (содержание) которых изменяется принудительно. Примером долгосрочного секрета является пароль. Краткосрочные секреты действуют в течение ограниченного времени их использования, например сеанса взаимодействия участников аутентификации, и, как правило, создаются автоматически. Примером краткосрочного секрета являются сеансовые ключи Kerberos

[1)] Определение термина «электронное удостоверение» приведено в ГОСТ Р 58833—2020 (пункт 3.62).

(см. [4]). Краткосрочные секреты, которые выдаются доверенной третьей стороной успешно аутентифицированному субъекту (объекту) доступа для использования, например в условиях временного отсутствия аутентификационного обмена между ними, считаются вторичными аутентификаторами.

3.5

аутентификация: Действия по проверке подлинности субъекта доступа и/или объекта доступа, а также по проверке принадлежности субъекту доступа и/или объекту доступа предъявленного идентификатора доступа и аутентификационной информации.

Примечание — Аутентификация рассматривается применительно к конкретному субъекту доступа и/или конкретному объекту доступа.

[ГОСТ Р 58833—2020, пункт 3.4]

Примечание — Совокупность идентификатора доступа и аутентификационной информации могут представлять собой электронное удостоверение в виде сертификата безопасности (цифрового сертификата) в формате, определенном в [5].

3.6

биометрические персональные данные: Сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность.

[Адаптировано из [6], статья 11]

3.7

взаимная аутентификация: Обоюдная аутентификация, обеспечивающая для каждого из участников процесса аутентификации, и субъекта доступа, и объекта доступа, уверенность в том, что другой участник процесса аутентификации является тем, за кого себя выдает.

[ГОСТ Р 58833—2020, пункт 3.10]

3.8

вторичная идентификация: Действия по проверке существования (наличия) идентификатора, предъявленного субъектом доступа при доступе, в перечне идентификаторов доступа, которые были присвоены субъектам доступа и объектам доступа при первичной идентификации.

Примечание — Вторичная идентификация рассматривается применительно к конкретному субъекту доступа.

[ГОСТ Р 58833—2020, пункт 3.12]

3.9

вычислительные ресурсы: Технические средства ЭВМ, в том числе процессор, объемы оперативной и внешней памяти, время, в течение которого программа занимает эти средства в ходе выполнения.

[ГОСТ 28195—89, приложение 1]

3.10

доверенная третья сторона: Участник процессов идентификации и аутентификации, предоставляющий одну или более услуг в области защиты информации, которому доверяют другие участники процессов идентификации и аутентификации как поставщику данных услуг.

Примечания

1 При идентификации и аутентификации доверенной третьей стороне доверяют и субъект доступа, и объект доступа.

2 В качестве доверенной третьей стороны могут рассматриваться: организация (например, осуществляющая функции центра сертификации), администратор автоматизированной (информационной) системы, устройство.

3 Доверенная третья сторона действует в полном соответствии с ожиданиями той стороны, которая пользуется ее услугами: и субъекта доступа, и объекта доступа или любого из них, при этом выполняя то, что она должна делать, и не выполняя то, что она не должна делать.

[Адаптировано из ГОСТ Р 58833—2020, пункт 3.15]

3.11

доступ: Получение одной стороной информационного взаимодействия возможности использования ресурсов другой стороны информационного взаимодействия.

Примечания

1 В качестве ресурсов стороны информационного взаимодействия, которые может использовать другая сторона информационного взаимодействия, рассматриваются информационные ресурсы, вычислительные ресурсы средств вычислительной техники и ресурсы автоматизированных (информационных) систем, а также средства вычислительной техники и автоматизированные (информационные) системы в целом.

2 Доступ к информации — возможность получения информации и ее использования.

[ГОСТ Р 58833—2020, пункт 3.17]

3.12

закрытый ключ неизвлекаемый (неизвлекаемый ключ): Закрытый ключ, который при его формировании и хранении невозможно извлечь из устройства аутентификации, в котором он был создан.

Примечание — Неизвлекаемость закрытого ключа заключается в отсутствии возможности его извлечения из устройства аутентификации, в котором он был создан, штатными средствами, предоставляемыми данным устройством аутентификации. Неизвлекаемость закрытого ключа в устройствах аутентификации, как правило, обеспечивается применяемыми схемотехническими решениями и гарантируется производителями устройств.

[Адаптировано из ГОСТ Р 58833—2020, пункт 3.19]

3.13

идентификатор доступа [субъекта (объекта) доступа], [идентификатор]: Признак субъекта доступа или объекта доступа в виде строки знаков (символов), который используется при идентификации и однозначно определяет (указывает) соотнесенную с ним идентификационную информацию.

[ГОСТ Р 58833—2020, пункт 3.20]

3.14

идентификационная информация: Совокупность значений идентификационных атрибутов, которая связана с конкретным субъектом доступа или конкретным объектом доступа.

Примечание — Идентификационная информация как совокупность значений идентификационных атрибутов, может быть, например, зарегистрирована в учетной записи субъекта (объекта) доступа, которая используется автоматизированной (информационной) системой.

[ГОСТ Р 70262.1—2022, пункт 3.12]

3.15

идентификация: Действия по присвоению субъектам и объектам доступа идентификаторов и (или) по сравнению предъявляемого идентификатора с перечнем присвоенных идентификаторов.

[[7], статья 3.3.9]

3.16

информационные ресурсы: Отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных, других информационных системах).

[ГОСТ Р 43.0.2—2006, статья 11]

3.17

ключ (key): Изменяемый параметр в виде последовательности символов, определяющий криптографическое преобразование.

[ГОСТ Р 34.12—2015, пункт 2.1.8]

3.18 **компрометация аутентификатора:** Нарушение конфиденциальности аутентификатора.

Примечание — Конфиденциальность аутентификатора может быть нарушена, например, раскрытием аутентификационной информации, составляющей секрет, утерей или хищением устройства аутентификации, содержащего аутентификационную информацию.

3.19

метод аутентификации: Реализуемое при аутентификации предопределенное сочетание факторов аутентификации, организации обмена и обработки аутентификационной информации, а также соответствующих данному сочетанию протоколов аутентификации.

[Адаптировано из ГОСТ Р 58833—2020, пункт 3.27]

3.20 **модуль безопасности (аппаратный модуль безопасности):** Сложно-функциональный блок (или совокупность сложно-функциональных блоков) микросхемы, или автономная микросхема в целом, или автономный программно-технический (аппаратный) комплекс, которые обеспечивают защиту размещенных и функционирующих в них приложений и данных от логических и/или физических атак.

Примечания

1 При аутентификации модуль безопасности используется для генерации (создания), хранения и управления криптографическими ключами, а также для выполнения криптографических преобразований и рассматривается как устройство аутентификации.

2 Аппаратный модуль безопасности может встраиваться в средства вычислительной техники (встраиваемый модуль безопасности), которые используют сервисы, предоставляемые модулем безопасности, либо подключаться к средствам вычислительной техники с применением согласованных интерфейсов (подключаемый модуль безопасности).

3.21

многофакторная аутентификация: Аутентификация, при выполнении которой используется не менее двух различных факторов аутентификации.

[ГОСТ Р 58833—2020, пункт 3.29]

3.22

объект доступа: Одна из сторон информационного взаимодействия, которая предоставляет доступ или к которой запрашивается и/или предоставляется (может быть предоставлен) доступ внешним по отношению к стороне информационного взаимодействия средством управления доступом.

Примечания

1 Примером использования внешнего средства управления доступом является диспетчер доступа среды функционирования, который является посредником при всех обращениях субъектов доступа к объектам доступа.

2 В качестве объектов доступа могут рассматриваться, например, информационные и вычислительные ресурсы средств вычислительной техники, ресурсы автоматизированных (информационных) систем, средства вычислительной техники и автоматизированные (информационные) системы в целом.

[Адаптировано из ГОСТ Р 58833—2020, пункт 3.33]

3.23

односторонняя аутентификация: Аутентификация, обеспечивающая только для одного из участников процесса аутентификации (объекта доступа) уверенность в том, что другой участник процесса аутентификации (субъект доступа) является тем, за кого себя выдает предъявленным идентификатором доступа.

[Адаптировано из ГОСТ Р 58833—2020, пункт 3.36]

3.24

однофакторная аутентификация: Аутентификация, при выполнении которой используется один фактор аутентификации.

[ГОСТ Р 58833—2020, пункт 3.37]

3.25

оператор автоматизированной (информационной) системы (оператор): Физическое лицо или юридическое лицо (организация), осуществляющее деятельность по эксплуатации автоматизированной (информационной) системы, в том числе по обработке содержащейся в ней информации.

[Адаптировано из ГОСТ Р 58833—2020, пункт 3.38]

3.26

первичная идентификация: Действия по формированию и регистрации информации о субъекте доступа или объекте доступа, а также действия по присвоению идентификатора доступа субъекту доступа или объекту доступа и его регистрации в перечне присвоенных идентификаторов доступа.

Примечание — Первичная идентификация рассматривается применительно к конкретному субъекту доступа и/или конкретному объекту доступа.

[ГОСТ Р 58833—2020, пункт 3.41]

3.27

подлинность: Свойство, определяющее, что фактический субъект или объект совпадает с заявленным.

[ГОСТ Р ИСО/МЭК 27000—2021, пункт 3.6]

3.28

протокол аутентификации: Протокол, позволяющий участникам процесса аутентификации осуществлять аутентификацию.

Примечания

1 Протокол реализует алгоритм (правила) аутентификационного обмена, в рамках которого субъект доступа и объект доступа последовательно выполняют определенные действия и обмениваются сообщениями, содержащими аутентификационную и/или другую информацию, используемую при аутентификации.

2 В криптографических протоколах аутентификации защита информации, используемой при аутентификации, реализуется с применением криптографических алгоритмов.

[Адаптировано из ГОСТ Р 58833 —2020, пункт 3.47]

3.29

простая аутентификация: Аутентификация с применением метода однофакторной односторонней аутентификации и соответствующих данному методу протоколов аутентификации.

[ГОСТ Р 58833 —2020, пункт 3.46]

3.30

процесс: Совокупность взаимосвязанных и (или) взаимодействующих видов деятельности, использующих входы для получения намеченного результата.

[ГОСТ Р ИСО 9000—2015, пункт 3.4.1]

3.31

ресурсы автоматизированной (информационной) системы (ресурсы): Средства, использующиеся (привлекаемые) в автоматизированной (информационной) системе для обработки информации (например, информационные, программные, технические, лингвистические).

[Адаптировано из [8], пункт А.20]

3.32

среда функционирования: Среда с предопределенными (установленными) граничными условиями, в которой существуют (функционируют) и взаимодействуют субъекты и объекты доступа.

Примечания

1 Область действия правил управления доступом рассматривается как предопределенное (установленное) граничное условие среды. При этом область действия правил управления доступом может быть реализована, например, в границах: одного или нескольких вычислительных процессов; одного или нескольких средств вычислительной техники; одной или нескольких автоматизированных (информационных) систем.

2 Граничные условия среды функционирования могут определяться, например, нормативными и правовыми документами, обладателем информации или оператором.

[Адаптировано из ГОСТ Р 58833—2020, пункт 3.53]

3.33

санкционирование доступа (авторизация): Предоставление субъекту доступа прав доступа, а также предоставление доступа в соответствии с установленными правилами управления доступом.

[Адаптировано из ГОСТ Р 58833—2020, пункт 3.50]

3.34 **средство аутентификации:** Устройство аутентификации, программа или их совокупность либо предмет (приспособление), которые вместе с аутентификационной информацией используются при аутентификации.

Примечания

1 Необходимость использования при аутентификации всех или отдельных составных частей средства аутентификации определяется его конструктивными особенностями и/или видом аутентификации. В некоторых случаях, когда отсутствует необходимость использования отдельных составных частей средства аутентификации (устройств, программ, предметов и т. п.), например при простой аутентификации по запоминаемому секрету, средство аутентификации может представлять собой аутентификатор. В других случаях средством аутентификации реализуется пользовательский интерфейс, который используется для получения (выбора) аутентификационной информации (например, одноразового пароля) либо для доступа и выполнения операций с аутентификационной информацией и другими данными, содержащимися в устройстве аутентификации [например, с электронным удостоверением в виде сертификата безопасности (цифрового сертификата)], а также для осуществления и (или) управления процессом аутентификации и, при необходимости, идентификации.

2 С целью предотвращения несанкционированного использования некоторые средства аутентификации (или устройства аутентификации из их состава) могут применяться по назначению только после их активации (перевода из неработоспособного состояния в работоспособное) посредством ввода необходимой для начала функционирования информации, например биометрических персональных данных владельца. При этом считается, что активация осуществляется с помощью второго фактора аутентификации.

3 При необходимости выделения особенностей средств аутентификации, используемых при соответствующих видах аутентификации, термин «средство аутентификации» может использоваться с общепринятыми уточнениями. Например, средство, используемое для строгой аутентификации (многофакторная, взаимная, с применением криптографических протоколов) может определяться как «многофакторное криптографическое средство аутентификации». При этом для выделения отдельных свойств средств аутентификации в термин могут включаться дополнительные уточнения, например «техническое» (совокупность электронных и механических частей) или «программное» (программа) средство аутентификации, или, например, средство аутентификации «с неизвлекаемым ключом» (неизвлекаемость закрытого ключа).

4 К техническим средствам аутентификации относятся как средства аутентификации, непосредственно представляющие собой технические устройства аутентификации или предметы (приспособления), так и средства, имеющие в своем составе технические устройства аутентификации.

3.35

строгая аутентификация: Аутентификация с применением метода многофакторной взаимной аутентификации и использованием только криптографических протоколов аутентификации.

[Адаптировано из ГОСТ Р 58833—2020, пункт 3.54]

3.36

субъект доступа: Одна из сторон информационного взаимодействия, которая инициирует получение и получает доступ.

Примечание — Субъектами доступа могут являться как физические лица (пользователи), так и ресурсы стороны информационного взаимодействия, а также вычислительные процессы, инициирующие получение и получающие доступ от их имени.

[ГОСТ Р 58833—2020, пункт 3.55]

3.37

уверенность: Убежденность в том, что оцениваемый объект будет функционировать в соответствии с заданным или установленным порядком (то есть корректно, надежно, эффективно, в соответствии с политикой безопасности).

[ГОСТ Р 54581—2011, пункт 2.18]

Примечание — Основанием для обоснованной уверенности являются воспроизводимые результаты определенных действий, которые необходимо выполнить при оценке.

3.38

уровень доверия: Оценочное значение по шкале, применяемой при получении воспроизводимых результатов определенных действий, которые необходимо выполнить для обеспечения уверенности в том, что оцениваемый объект соответствует установленным требованиям.

Примечания

1 Уровень доверия не измеряется количественными показателями.

2 Уровень доверия обычно определяется усилиями, затраченными на выполнение определенных действий.

[Адаптировано из ГОСТ Р 54581—2011, пункт 2.10]

Примечание — Оценочная шкала имеет следующий порядок (от меньшего к большему, слева направо): низкий уровень доверия, средний уровень доверия, высокий уровень доверия.

3.39

усиленная аутентификация: Аутентификация с применением метода многофакторной односторонней или многофакторной взаимной аутентификации и соответствующих данному методу протоколов аутентификации, в том числе криптографических.

[Адаптировано из ГОСТ Р 58833—2020, пункт 3.59]

3.40

устройство аутентификации: Техническое (физическое) или виртуальное устройство или предмет, предназначенное для создания (генерации), хранения и предоставления информации, которая используется при идентификации и/или аутентификации владельца устройства.

[Адаптировано из ГОСТ Р 58833—2020, пункт 3.60]

Примечания

1 Устройство аутентификации может иметь как все указанные функции, так и обладать ограниченным их набором, а также может выполнять и другие функции, например управлять доступом к информации, содержащейся в устройстве.

2 Техническое устройство аутентификации включает физическую (реальную) техническую (аппаратную) платформу (как правило, на базе микросхемы) и встроенные системные и прикладные программы, функционирующие на данной платформе. Функциональное назначение технического устройства аутентификации реализуется встроенными прикладными программами.

3 Виртуальное устройство аутентификации представляет собой кажущееся реально существующим техническое устройство, поскольку все его функции реализуются какими-либо другими устройствами и (или) программами.

4 Технические устройства аутентификации не используют при функционировании вычислительные ресурсы средств вычислительной техники и считаются функционально отделенными от средств вычислительной техники независимо от их конструкции.

3.41

фактор: Вид (форма) существования информации, используемой для идентификации и аутентификации.

Примечание — Допускается уточнять термин сообразно его конкретному использованию. Например, применительно к аутентификации, допускается использовать термин «фактор аутентификации».

[ГОСТ Р 58833—2020, пункт 3.61]

4 Общие положения

4.1 В соответствии с ГОСТ Р 58833 процесс аутентификации при доступе субъекта доступа к объекту доступа должен включать в себя действия по проверке подлинности субъекта (объекта[1)]) доступа, а также принадлежности субъекту (объекту) доступа предъявленного при проверке идентификатора и аутентификационной информации.

Примечание — При доступе субъекта доступа к объекту доступа аутентификация следует за процессом вторичной идентификации при каждом запросе субъекта на доступ и осуществляется в случае положительного результата вторичной идентификации по ГОСТ Р 70262.1.

При аутентификации доказательство подлинности субъекта (объекта) доступа должно основываться на проверке соответствия аутентификационной информации, предъявленной субъектом (объектом) доступа, и аутентификационной информации, которая ассоциирована с предъявленным идентификатором доступа у объекта (субъекта) доступа.

Доказательство принадлежности субъекту (объекту) идентификатора и аутентификационной информации должно основываться на проверке актуальности аутентификационной информации и проверке связи идентификатора и аутентификационной информации с субъектом (объектом) доступа.

4.2 Целью аутентификации является формирование необходимой уверенности в том, что субъект (объект) доступа действительно является тем зарегистрированным субъектом (объектом) доступа, за которого себя выдает предъявленным идентификатором доступа.

4.3 В процессе аутентификации применяются следующие факторы: фактор знания, фактор владения, биометрический фактор. При доступе к объекту доступа для аутентификации субъекта доступа необходимо использовать один фактор (при однофакторной аутентификации) или одновременно не менее двух различных факторов (при многофакторной аутентификации).

Примечание — Общая характеристика факторов, используемых при аутентификации, и правила их использования определяются ГОСТ Р 58833.

4.4 Аутентификация осуществляется в рамках аутентификационного обмена между участниками процесса аутентификации — субъектом доступа, доверенной третьей стороной (при использовании ее услуг) и объектом доступа — с учетом их следующих функциональных ролей:

- доказывающая сторона. Основной задачей доказывающей стороны является доказательство ее подлинности, в том числе подтверждение того, что она обладает (контролирует) и способна распоряжаться аутентификатором;
- доверяющая сторона. Основной задачей доверяющей стороны является проверка подлинности доказывающей стороны, а также проверка, при необходимости, утверждения (доказательства) доказывающей стороны, что она обладает (контролирует) и способна распоряжаться аутентификатором;
- проверяющая сторона. Основной задачей проверяющей стороны является проверка принадлежности доказывающей стороне идентификатора доступа и аутентификатора, которые зафиксированы за ней регистрирующей стороной, а также предоставление доверяющей стороне подтверждения (или опровержения) по результатам проверки.

Примечание — Регистрирующая сторона[2)] не принимает непосредственного участия в аутентификации, но при первичной идентификации формирует и присваивает субъекту (объекту) доступа и регистрирует аутентификационную информацию, которая используется при аутентификационном обмене.

4.5 Для организации аутентификационного обмена используются подтверждающая информация, которая имеется у доказывающей и проверяющей сторон, и проверочная информация, которая имеется у доверяющей и проверяющей сторон[3)] (см. рисунок 1). На основе подтверждающей и проверочной информации в соответствии с используемым протоколом аутентификации формируется (см. рисунок 2) передаваемая информация, которой в виде сообщений обмениваются стороны в процессе аутентификации (см. рисунки 1, 2).

[1)] Проверка подлинности объекта доступа и все соответствующие данной проверке действия осуществляются при взаимной аутентификации субъекта и объекта доступа.

[2)] Назначение и функции регистрирующей стороны определены в ГОСТ Р 58833 и ГОСТ Р 70262.1.

[3)] Порядок и правила формирования, распределения между сторонами, а также доставки и получения сторонами подтверждающей и проверочной информации, необходимой при аутентификации, не являются предметом рассмотрения настоящего стандарта.

Примечания

1 Подтверждающая информация используется для подтверждения подлинности доказывающей стороны. Как правило, в качестве подтверждающей информации при аутентификационном обмене используется аутентификационная информация. Примерами подтверждающей информации являются: пароль; секретный ключ, используемый при аутентификации с применением симметричных криптографических алгоритмов; закрытый ключ, используемый при аутентификации с применением асимметричных криптографических алгоритмов.

2 Проверочная информация применяется при верификации принятой подтверждающей информации проверяющей стороной. Как правило, в качестве проверочной информации при аутентификационном обмене используется аутентификационная информация. Примерами проверочной информация являются: пароль; секретный ключ, используемый при аутентификации с применением симметричных криптографических алгоритмов; открытый ключ, используемый при аутентификации с применением асимметричных криптографических алгоритмов. При аутентификации доверяющей стороной (например, объектом доступа) доказывающей стороны (например, субъекта доступа) в условиях отсутствия возможности аутентификационного обмена с проверяющей стороной (доверенной третьей стороной) проверочная информация может представлять собой, например, список отозванных сертификатов, распространяемый доверенной третьей стороной как проверяющей стороной.

3 Передаваемая информация для сеанса аутентификации формируется на основе, например, уникального идентификатора доказывающей стороны, уникального идентификатора проверяющей стороны, типа аутентификационного обмена; типа подтверждающей информации (например, пароль или закрытый ключ), значения подтверждающей информации (например, значение пароля), типа передаваемой информации и т. п. Передаваемая информация может включать статус аутентификационного обмена (успех, сбой и т. п.), результат преобразования подтверждающей информации, выполненного по правилам, которые определяются используемым протоколом аутентификации, или результат совместного преобразования подтверждающей информации и других данных (например, значения времени, случайного числа, уникального идентификатора проверяющей стороны и т. п.).

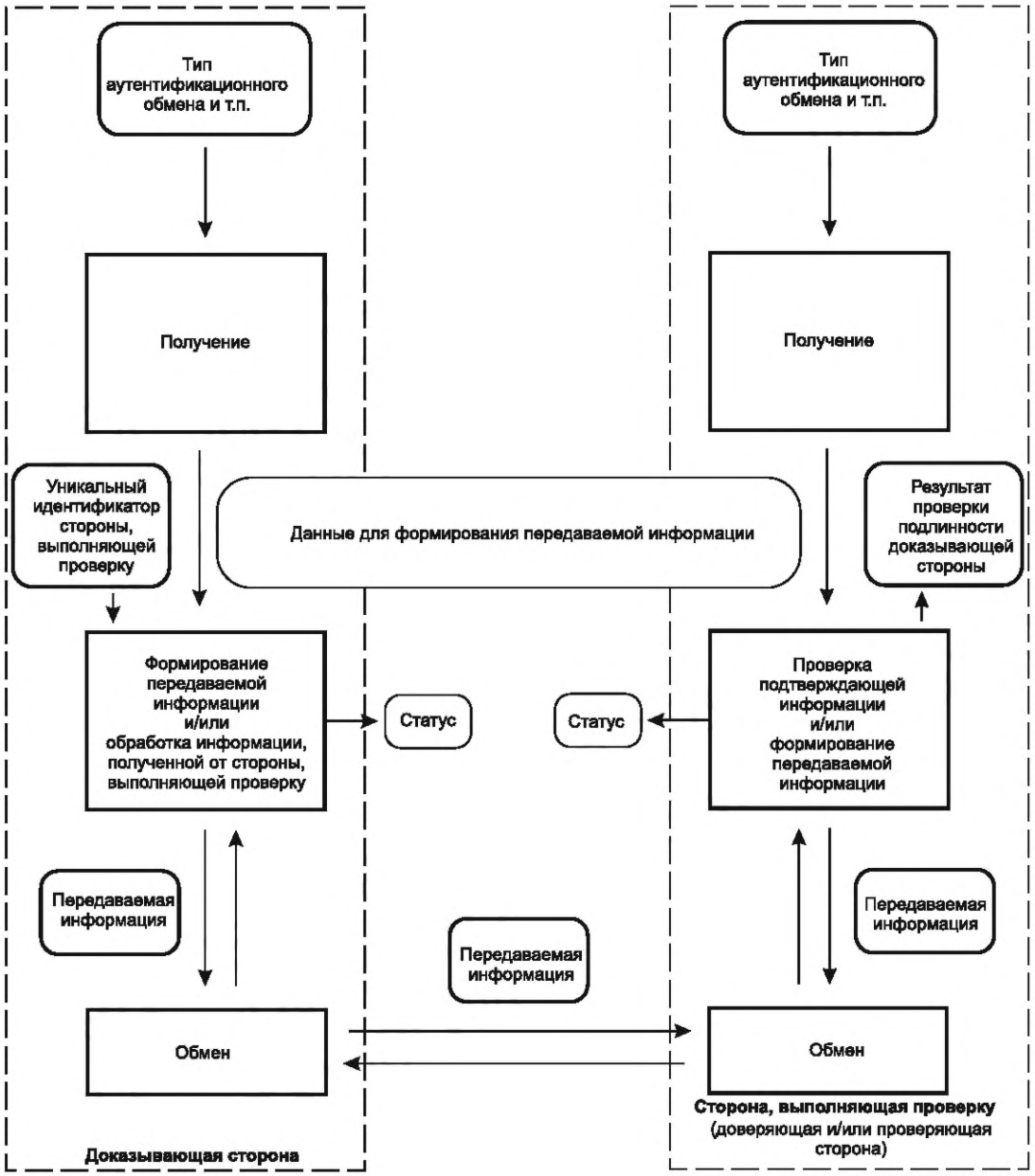


Примечания

1 На рисунке 1 роли участников процесса аутентификации приведены для аутентификации с участием доверенной третьей стороны в режиме реального времени. При взаимной аутентификации субъект и объект доступа поочередно выполняют роль доказывающей и доверяющей сторон.

2 На рисунке 1 передача проверочной информации от доверенной третьей стороны (проверяющей стороны) объекту доступа (доверяющей стороне) осуществляется для выполнения автономной (локальной) аутентификации объектом доступа (доверяющей и проверяющей стороной) субъекта доступа (доказывающей стороны) или для выполнения аутентификации в условиях временного отсутствия взаимодействия между доверенной третьей стороной и объектом доступа. Для автономной (локальной) аутентификации в качестве проверочной информации может использоваться долгосрочный секрет, например пароль, назначаемый администратором автоматизированной (информационной) системы (доверенной третьей стороной) пользователю (субъекту доступа) на конкретных автономных средствах вычислительной техники. При аутентификации в условиях отсутствия возможности аутентификационного обмена с доверенной третьей стороной в качестве проверочной информации могут использоваться вторичные аутентификаторы, которые предварительно получаются от сетевой службы аутентификации домена (доверенной третьей стороны), например сеансовые ключи Kerberos, либо открытая информация, например список отозванных сертификатов.

Рисунок 1 — Взаимосвязь между участниками процесса аутентификации с учетом их функциональных ролей и информации, используемой при аутентификации



Примечание — На рисунке 2 указано, что получение данных для формирования передаваемой информации осуществляется и доказывающей стороной, и стороной выполняющей проверку. На практике, при аутентификации, получение данных выполняется либо одной из сторон, либо не выполняется ни одной.

Рисунок 2 — Пример формирования передаваемой информации на основе подтверждающей, проверочной и другой информации, необходимой для осуществления аутентификационного обмена

4.6 В общем случае процесс аутентификации, с учетом результатов первичной и вторичной идентификации, должен включать:

а) формирование и регистрацию аутентификатора субъекта (объекта) доступа при первичной идентификации регистрирующей стороной. При этом аутентификатор может назначаться регистрирующей стороной субъекту (или субъекту и объекту) доступа или самостоятельно формироваться субъектом доступа в соответствии с установленными правилами;

б) хранение и поддержание в актуальном состоянии (обновление) аутентификационной информации регистрирующей стороной и субъектом (объектом) доступа;

в) запрос доступа субъектом доступа к объекту доступа и его вторичная идентификация;

г) аутентификацию субъекта доступа (при условии успешной вторичной идентификации) и, при необходимости, объекта доступа (см. рисунок 3), в том числе:

1) проверку доверяющей стороной подлинности доказывающей стороны. Проверка осуществляется путем представления доказывающей стороной аутентификатора и последующего контроля доверяющей стороной соответствия предъявленного аутентификатора доказывающей стороны аутентификатору, имеющемуся у доверяющей стороны, либо путем обмена аутентификаторами и другими данными, необходимыми для взаимной аутентификации в соответствии с протоколом аутентификации, между доказывающей и доверяющей сторонами. Дополнительно доказывающая сторона при необходимости и (или) по запросу доверяющей стороны должна подтвердить, что осуществляет контроль над аутентификатором и способна им распоряжаться.

Примечание — Для подтверждения того, что доказывающая сторона осуществляет контроль, например, над запоминаемым или поисковым секретом и способна им распоряжаться, может использоваться внеполосный секрет (подробно средства аутентификации рассмотрены в 5.6), а для подтверждения того, что доказывающая сторона осуществляет контроль, например, над устройством аутентификации, которое содержит аутентификационную информацию, может использоваться PIN[1)]-код. Как правило проверка того, что доказывающая сторона контролирует аутентификатор и способна им распоряжаться, выполняется для субъектов доступа, ассоциированных с физическими лицами (пользователями),

2) проверку проверяющей стороной по запросу доверяющей стороны принадлежности доказывающей стороне предъявленного аутентификатора, включая проверку актуальности (действительности) аутентификационной информации и проверку связи аутентификатора с доказывающей стороной. По результатам проверки проверяющая сторона предоставляет либо не предоставляет доверяющей стороне подтверждение актуальности идентификатора и аутентификатора, а также подтверждение наличия связи с доказывающей стороной в установленном протоколом аутентификации виде;

д) принятие доверяющей стороной решения о результате аутентификации и доведение решения доказывающей стороне. Дополнительно для доказывающей стороны — субъекта доступа — с учетом предъявленного аутентификатора доверяющей стороной определяется возможность выполнения запрошенных действий (операций) при последующем проведении авторизации.

Примечание — Возможность выполнения запрошенных действий (операций) при использовании конкретного аутентификатора, как правило, определяется соответствием уровня доверия аутентификации для используемого аутентификатора уровню доверия, необходимому для запрошенных действий (операций) субъекта доступа в отношении объекта доступа.

4.7 В общем случае при аутентификации объект доступа выполняет регистрацию, хранит и поддерживает в актуальном состоянии аутентификационную информацию, осуществляет проверку подлинности субъекта доступа, принадлежности ему аутентификатора, а также проверяет способность субъекта доступа распоряжаться аутентификатором. При этом субъект доступа подтверждает (доказывает) свою подлинность и владение аутентификатором. В этом случае все действия осуществляются непосредственно субъектом и объектом доступа. Объект доступа объединяет функциональные роли регистрирующей, проверяющей, доверяющей сторон (при односторонней аутентификации) и дополнительно может иметь роль доказывающей стороны (при взаимной аутентификации), а субъект доступа имеет функциональную роль доказывающей стороны (при односторонней аутентификации) и дополнительно может иметь роли проверяющей и доверяющей сторон (при взаимной аутентификации).

При участии доверенной третьей стороны в процессе аутентификации она осуществляет регистрацию субъекта (объекта) доступа, а также по запросу проверяет принадлежность аутентификатора субъекту (объекту) доступа. В данном случае все действия осуществляются субъектом доступа, объектом доступа и доверенной третьей стороной. При этом доверенная третья сторона объединяет функциональные роли регистрирующей и проверяющей сторон, объект доступа — функциональную роль доверяющей стороны (при односторонней аутентификации) и дополнительно может иметь роль доказывающей стороны (при взаимной аутентификации), а субъект доступа — функциональную роль доказывающей стороны (при односторонней аутентификации) и дополнительно может иметь роль доверяющей стороны (при взаимной аутентификации).

[1)] PIN-код — персональный идентификационный номер (personal identification number).



Рисунок 3 — Общая схема взаимодействия сторон при аутентификации

4.8 Необходимость аутентификации устанавливается как для субъектов доступа, которые являются физическими лицами, так и для субъектов (объектов) доступа, которые представляют собой информационные и вычислительные ресурсы. Аутентификация должна осуществляться с учетом данных особенностей субъектов (объектов) доступа, а также с учетом возможности использования и применимости положений настоящего стандарта для конкретной среды функционирования.

4.9 Участники процесса аутентификации должны обеспечивать защиту информации, используемой при аутентификации. При этом состав и содержание мер защиты, в том числе мер защиты с применением криптографических методов (алгоритмов), в конкретной среде функционирования должны определяться в соответствии с нормативными правовыми актами и документами по стандартизации.

5 Виды и средства аутентификации

5.1 Аутентификация осуществляется в порядке и по правилам, определяемым видом аутентификации с применением соответствующих средств аутентификации.

5.2 В соответствии с ГОСТ Р 58833 при организации доступа должен использоваться один или несколько видов аутентификации: простая, усиленная или строгая.

5.3 Простой аутентификацией должна считаться однофакторная односторонняя аутентификация с организацией передачи аутентификационной информации при аутентификационном обмене от субъекта доступа к объекту доступа. В процессе простой аутентификации необходимо использовать протоколы аутентификации, соответствующие данной организации передачи аутентификационной информации, в том числе криптографические.

5.4 Усиленной аутентификацией должна считаться многофакторная односторонняя аутентификация с организацией передачи аутентификационной информации при аутентификационном обмене от субъекта доступа к объекту доступа или многофакторная взаимная аутентификация с организацией аутентификационного обмена между субъектом доступа и объектом доступа. При усиленной аутентификации необходимо использовать протоколы аутентификации, соответствующие данной организации передачи аутентификационной информации в рамках аутентификационного обмена, в том числе криптографические.

5.5 Строгой аутентификацией должна считаться многофакторная взаимная аутентификация с организацией двухстороннего, между субъектом доступа и объектом доступа, или многостороннего,

между субъектом доступа, объектом доступа и третьей доверенной стороной, аутентификационного обмена. В процессе строгой аутентификации должны использоваться только криптографические протоколы аутентификации, соответствующие данной организации передачи аутентификационной информации в рамках аутентификационного обмена.

5.6 При аутентификации необходимо использовать средства аутентификации (аутентификаторы), характеристики которых приведены в 5.6.1—5.6.10.

Примечание — Конкретные реализации средств и устройств аутентификации, а также способы их применения в среде функционирования не являются предметом рассмотрения данного национального стандарта.

5.6.1 Запоминаемый секрет. Аутентификатор, обычно называемый паролем или, если это числовое значение — PIN-кодом, является секретным значением для запоминания субъектом доступа (доказывающей стороной). Если регистрирующая (доверяющая или проверяющая) сторона заносит выбранный запоминаемый секрет на основе некоторых его параметров в список скомпрометированных аутентификаторов, субъект доступа (доказывающая сторона) должен выбрать другой запоминаемый секрет. При аутентификации с помощью данного средства аутентификации используется фактор знания — подтверждается знание запоминаемого секрета.

Примечания

1 Условия использования запоминаемых секретов (например, сложность и длительность действия) могут устанавливаться нормативными правовыми или методическими документами, обладателем информации или оператором.

2 В список скомпрометированных аутентификаторов, как правило, заносятся запоминаемые секреты, которые могли стать доступными лицам, не являющимся их владельцами, и (или) процессам, которые получили к ним несанкционированный доступ. В качестве параметров, на основе которых запоминаемые секреты считаются скомпрометированными, может рассматриваться, например, нарушение конфиденциальности вследствие наступления таких событий как хищение, утрата, разглашение, раскрытие, разгадывание и т. п.

5.6.2 Поисковый секрет. Поисковый секрет представляет собой физическую или электронную запись на носителе, в которой хранится совокупность секретов (аутентификаторов), например одноразовых паролей, формируемых для субъекта доступа регистрирующей стороной. Субъект доступа (доказывающая сторона) использует средство аутентификации для поиска секрета (аутентификатора), необходимого для ответа на запрос доверяющей (или проверяющей) стороны. При аутентификации с помощью данного средства аутентификации используется фактор владения — подтверждается владение носителем и контроль над ним (способность им распоряжаться).

Примечание — Примерами поисковых секретов являются шифр-блокнот, скрэтч-карта.

5.6.3 Внеполосный секрет («второй канал»). Средство аутентификации представляет собой устройство, которое имеет уникальный (для используемой среды функционирования) адрес и для получения секрета может взаимодействовать с доверяющей (или проверяющей) стороной по отдельному каналу передачи данных, называемому дополнительным («вторым») каналом. Субъект доступа (доказывающая сторона) обладает устройством, а доверяющая (или проверяющая) сторона обеспечивает функционирование сервиса, который при аутентификации поддерживают обмен по этому «дополнительному» каналу, физически отделенному от «основного» канала передачи данных. При аутентификации с помощью данного средства аутентификации используется фактор владения — подтверждается владение устройством и контроль над ним (способность им распоряжаться).

Примечание — Секрет, полученный по дополнительному каналу, применяется совместно с другими аутентификаторами, например с запоминаемым секретом. Чаще всего для получения внеполосного секрета используется пользовательское (оконечное) устройство подвижной радиотелефонной связи (мобильной связи) любого вида, например смартфон.

5.6.4 Однофакторный генератор одноразовых паролей (OTP[1])-генератор). Однофакторный генератор одноразовых паролей формирует динамически изменяющиеся одноразовые пароли (секреты) для аутентификации. Представляет собой техническое устройство или программу (программный

[1]) OTP — одноразовый пароль (one time password).

генератор)[1], отделенные от средств вычислительной техники, на которых (с помощью которых)[2] осуществляется аутентификация. В качестве источника для формирования динамически изменяющихся одноразовых паролей (секретов) используется встроенный секрет или одноразовый код, который может быть сформирован по текущему времени или по событию (например, нажатию кнопки на устройстве) или исходя из текущего значения счетчика на устройстве у доказывающей стороны и значения счетчика у доверяющей стороны. Сформированный одноразовый пароль (секрет) передается субъектом доступа (доказывающей стороной) доверяющей стороне для проверки. Однофакторные генераторы одноразовых паролей аналогичны средствам аутентификации с поисковым секретом за исключением того, что секреты независимо формируются доказывающей и доверяющей сторонами и сравниваются доверяющей стороной. Однофакторный генератор одноразовых паролей не требует активации для функционирования. При аутентификации с помощью данного средства аутентификации используется фактор владения — подтверждается владение устройством (программой) и контроль над ним (способность им распоряжаться).

5.6.5 Многофакторный генератор одноразовых паролей. Многофакторный генератор одноразовых паролей формирует динамически изменяющиеся одноразовые пароли (секреты) для аутентификации после активации с помощью дополнительного фактора аутентификации. Представляет собой техническое устройство или программу (программный генератор), отделенные от средств вычислительной техники, на которых (с помощью которых) осуществляется аутентификация, и функционирует аналогично однофакторному генератору одноразовых паролей. Второй фактор аутентификации может представлять собой информацию, полученную с клавиатуры (пароль, PIN-код и т. п.) и/или биометрического сканера (биометрические персональные данные) средств вычислительной техники или устройства. При аутентификации с помощью данного средства аутентификации используются фактор владения — подтверждается владение устройством (программой) и контроль над ним (способность им распоряжаться) — совместно с фактором знания (подтверждается знание секрета) и/или с биометрическим фактором (подтверждается соответствие биометрических персональных данных).

5.6.6 Однофакторное криптографическое программное средство аутентификации. Представляет собой криптографические ключи и программу, осуществляющую криптографические преобразования, которые хранятся на носителе и функционируют в составе средств вычислительной техники или аналогичных устройств. Выходные данные средства аутентификации зависят от используемого криптографического протокола аутентификации и являются установленным видом сообщения аутентификационного обмена. При аутентификации с помощью данного средства аутентификации используется фактор владения — подтверждается владение криптографическими ключами и контроль над ними (способность ими распоряжаться).

5.6.7 Однофакторное криптографическое техническое средство аутентификации. Представляет собой совокупность отделенного от средств вычислительной техники технического устройства аутентификации с криптографическими ключами и программы в составе средств вычислительной техники, осуществляющей криптографические преобразования и/или реализующей взаимодействие с устройством аутентификации. Устройство аутентификации осуществляет хранение самостоятельно выработанных и/или импортированных в него криптографических ключей, а также выполняет криптографические преобразования с их использованием и предоставляет результаты или представляет криптографические ключи для выполнения криптографических преобразований программой средства аутентификации через непосредственное (прямое) соединение устройства аутентификации со средствами вычислительной техники. Выходные данные средства аутентификации зависят от используемого криптографического протокола аутентификации и являются установленным видом сообщения аутентификационного обмена. При аутентификации с помощью данного средства аутентификации используется фактор владения — подтверждается владение криптографическими ключами и контроль над ними (способность ими распоряжаться).

---

[1] Программный генератор динамически изменяющихся паролей (программный OTP-генератор) может функционировать на различных средствах вычислительной техники, например, на мобильном устройстве (смартфоне) или на планшетном, мобильном, портативном, стационарном компьютере.

[2] Здесь и далее понимается, например, использование средств вычислительной техники при аутентификации пользователя на удаленных средствах вычислительной техники или в удаленных автоматизированных (информационных) системах, доступ к которым осуществляется с использованием телекоммуникационных технологий. В данном случае программный генератор одноразовых паролей может входить в состав средств вычислительной техники, с помощью которых осуществляется аутентификация пользователя на удаленных средствах вычислительной техники.

5.6.8 Многофакторное криптографическое программное средство аутентификации. Представляет собой криптографические ключи и программу, осуществляющую криптографические преобразования, которые хранятся на носителе и функционируют в составе средств вычислительной техники или аналогичных устройств. Доступ к криптографическим ключам осуществляется с использованием второго фактора аутентификации. Второй фактор аутентификации может представлять собой информацию, полученную с клавиатуры (секрет: пароль, PIN-код и т. п.) или биометрического сканера (биометрические персональные данные) средств вычислительной техники, либо совокупность данной информации. Выходные данные средства аутентификации зависят от используемого криптографического протокола аутентификации и являются установленным видом сообщения аутентификационного обмена. При аутентификации с помощью данного средства аутентификации используются фактор владения [подтверждаются контроль (владение) и способность распоряжаться криптографическими ключами] совместно с фактором знания (подтверждается знание секрета) и/или с биометрическим фактором (подтверждается соответствие биометрических персональных данных).

5.6.9 Многофакторное криптографическое техническое средство аутентификации. Представляет собой совокупность отделенного от средств вычислительной техники технического устройства аутентификации с криптографическими ключами и программы в составе средств вычислительной техники, осуществляющей криптографические преобразования и/или реализующей взаимодействие с устройством аутентификации. Устройство аутентификации осуществляет хранение самостоятельно выработанных и/или импортированных в него криптографических ключей, а также выполняет, при необходимости, криптографические преобразования с их использованием и представляет результаты или предоставляет криптографические ключи для выполнения криптографических преобразований программой средства аутентификации через непосредственное (прямое) соединение устройства аутентификации со средствами вычислительной техники. Доступ к криптографическим ключам и/или результатам криптографических преобразований осуществляется после активации устройства с помощью второго фактора аутентификации. Второй фактор аутентификации может представлять собой информацию, полученную с клавиатуры средств вычислительной техники или устройства аутентификации (секрет: пароль, PIN-код и т. п.), либо информацию с биометрического сканера средств вычислительной техники или устройства аутентификации (биометрические персональные данные), либо совокупность данной информации. Выходные данные средства аутентификации зависят от используемого криптографического протокола аутентификации и являются установленным видом сообщения аутентификационного обмена. При аутентификации с помощью данного средства аутентификации используется фактор владения [подтверждаются контроль (владение) и способность распоряжаться криптографическими ключами] совместно с фактором знания (подтверждается знание секрета) и/или с биометрическим фактором (подтверждается соответствие биометрических персональных данных).

5.6.10 Многофакторное криптографическое техническое средство аутентификации с неизвлекаемыми ключами. Представляет собой совокупность отделенного от средств вычислительной техники технического устройства аутентификации с криптографическими ключами и программы в составе средств вычислительной техники, осуществляющей криптографические преобразования и/или реализующей взаимодействие с устройством аутентификации. Устройство аутентификации самостоятельно вырабатывает и хранит закрытые неизвлекаемые криптографические ключи, а также выполняет криптографические преобразования с их использованием и представляет результаты через непосредственное (прямое) соединение устройства аутентификации со средствами вычислительной техники. Использование криптографических ключей и/или представление результатов осуществляется после активации устройства с помощью второго фактора аутентификации. Второй фактор аутентификации может представлять собой информацию, полученную с клавиатуры средств вычислительной техники или устройства аутентификации (секрет: пароль, PIN-код и т. п.), либо информацию с биометрического сканера средств вычислительной техники или устройства аутентификации (биометрические персональные данные), либо совокупность данной информации. Выходные данные средства аутентификации зависят от используемого криптографического протокола аутентификации и являются установленным видом сообщения аутентификационного обмена. При аутентификации с помощью данного средства аутентификации используется фактор владения [подтверждаются контроль (владение) и способность распоряжаться криптографическими ключами] совместно с фактором знания (подтверждается знание секрета) и/или с биометрическим фактором (подтверждается соответствие биометрических персональных данных).

5.7 Субъекты доступа, ассоциированные с физическими лицами, в зависимости от вида аутентификации могут использовать при аутентификации все вышеперечисленные средства аутентификации,

а субъекты и объекты доступа, ассоциированные со средствами вычислительной техники, могут использовать при аутентификации криптографические технические средства аутентификации.

Примечания

1 Технические средства аутентификации, имеющие в своем составе технические устройства аутентификации, например устройства аутентификации типоразмера (форм-фактора) «Смарт-карта» или «USB-ключ», как правило, используются при аутентификации их владельцев — физических лиц как пользователей средств вычислительной техники или пользователей автоматизированных (информационных) систем.

2 Технические средства аутентификации, имеющие в своем составе технические устройства аутентификации, встроенные в средства вычислительной техники, например встроенные аппаратные модули безопасности, как правило, используются при аутентификации средств вычислительной техники в рамках информационного взаимодействия с другими средствами вычислительной техники.

6 Уровни доверия аутентификации

6.1 Уровень доверия аутентификации определяет достигнутую уверенность в том, что субъект (объект) доступа, успешно прошедший идентификацию и аутентификацию, действительно является тем зарегистрированным субъектом (объектом) доступа, за которого себя выдает предъявленным идентификатором доступа.

Примечание — В соответствии с ГОСТ Р 70262.1 уверенность в том, что субъект доступа, успешно прошедший идентификацию, действительно соответствует зарегистрированной идентификационной информации, которая однозначно соотносится с предъявленным идентификатором доступа, определяется уровнем доверия идентификации.

Уровень доверия аутентификации определяет необходимые к применению вид аутентификации и средства аутентификации (или совокупность средств аутентификации).

6.2 Устанавливаются три уровня доверия аутентификации (также см. таблицу А.1).

6.2.1 Низкий уровень доверия. На данном уровне доверия имеется некоторая уверенность в том, что субъект доступа, успешно прошедший идентификацию и аутентификацию, действительно является тем зарегистрированным субъектом доступа, за которого себя выдает предъявленным идентификатором доступа. При этом субъект доступа должен иметь и контролировать аутентификатор, который используется в средствах аутентификации, реализующих применение фактора знания или фактора владения при аутентификации.

На низком уровне доверия аутентификации является достаточным использование простой аутентификации с применением одного, любого из следующих средств аутентификации: запоминаемого секрета, поискового секрета, однофакторного генератора одноразовых паролей, однофакторного криптографического программного средства аутентификации, однофакторного криптографического технического средства аутентификации.

По решению оператора для обеспечения в конкретной среде функционирования низкого уровня доверия наряду с указанными видом аутентификации и перечнем средств аутентификации, может использоваться усиленная или строгая аутентификация с применением одного, любого из следующих средств аутентификации: многофакторного генератора одноразовых паролей, многофакторного криптографического программного средства аутентификации, многофакторного криптографического технического средства аутентификации, многофакторного криптографического технического средства аутентификации с неизвлекаемым ключом.

6.2.2 Средний уровень доверия. На данном уровне доверия появляется умеренная уверенность в том, что субъект доступа[1)], успешно прошедший идентификацию и аутентификацию, действительно является тем зарегистрированным субъектом доступа, за которого себя выдает предъявленным идентификатором доступа. При этом субъект доступа должен иметь и контролировать аутентификатор, который используется в средствах аутентификации, реализующих применение не менее двух различных факторов при аутентификации.

На среднем уровне доверия аутентификации необходимо использование усиленной аутентификации с применением следующих средств аутентификации: многофакторного генератора одноразовых паролей или запоминаемого секрета, используемого совместно с поисковым секретом, или внеполосным секретом, или однофакторным генератором одноразовых паролей.

[1)] При использовании на среднем уровне доверия взаимной аутентификации — субъект доступа и объект доступа.

По решению оператора для обеспечения в конкретной среде функционирования среднего уровня доверия наряду с указанными видом аутентификации и перечнем средств аутентификации (или их совокупностью) может использоваться строгая аутентификация с применением одного, любого из следующих средств: многофакторного криптографического программного средства, многофакторного криптографического технического средства аутентификации, многофакторное криптографическое техническое средство аутентификации с неизвлекаемым ключом, а также может использоваться строгая аутентификация с применением запоминаемого секрета совместно с однофакторным криптографическим программным средством аутентификации или однофакторным криптографическим техническим средством аутентификации.

6.2.3 Высокий уровень доверия. На данном уровне доверия достигается значительная уверенность в том, что и субъект доступа, успешно прошедший идентификацию и аутентификацию, и объект доступа, успешно прошедший аутентификацию, действительно являются теми зарегистрированными субъектом и объектом доступа, за которого себя выдает каждый из них. При этом субъект (объект) доступа должен иметь и контролировать аутентификатор, который используется в технических средствах аутентификации, реализующих применение не менее двух различных факторов при аутентификации.

На высоком уровне доверия аутентификации должны использоваться технические средства аутентификации (при совместном использовании нескольких средств аутентификации как минимум одно из них должно быть техническим), реализующие строгую аутентификацию: многофакторное криптографическое техническое средство аутентификации, или однофакторное криптографическое техническое средство аутентификации совместно с запоминаемым секретом, или многофакторный генератор одноразовых паролей (техническое устройство или программный генератор) совместно с однофакторным криптографическим техническим средством аутентификации, или многофакторный генератор одноразовых паролей (техническое устройство) совместно с однофакторным криптографическим программным средством аутентификации, или однофакторный генератор одноразовых паролей (техническое устройство) совместно с многофакторным криптографическим программным средством аутентификации, или однофакторный генератор одноразовых паролей (техническое устройство) совместно с однофакторным криптографическим программным средством аутентификации и запоминаемым секретом.

Для достижения на данном уровне доверия максимальной уверенности технические средства аутентификации, осуществляющие строгую аутентификацию, должны использовать криптографические алгоритмы с неизвлекаемыми ключами, реализованные в многофакторном криптографическом техническом средстве аутентификации с неизвлекаемыми ключами.

6.3 Уровень доверия аутентификации, который необходимо достигнуть в конкретной среде функционирования, должен устанавливаться на основе ГОСТ Р 58833 в соответствии с нормативными правовыми документами и/или с учетом результатов анализа рисков информационной безопасности, выполняемого в соответствии с ГОСТ Р ИСО/МЭК 27005.

Приложение А
(справочное)

Общая характеристика уровней доверия аутентификации

Таблица А.1 — Уровни доверия аутентификации

Уровень доверия аутентификации	Уверенность в результатах аутентификации	Виды аутентификации	Средства аутентификации
Низкий уровень доверия аутентификации	Некоторая уверенность в том, что субъект доступа, успешно прошедший идентификацию и аутентификацию, действительно является тем зарегистрированным субъектом доступа, за которого себя выдает предъявленным идентификатором доступа при условии, что субъект доступа имеет и контролирует аутентификатор	Простая аутентификация	Запоминаемый секрет, или поисковый секрет, или однофакторный генератор одноразовых паролей, или однофакторное криптографическое программное средство аутентификации, или однофакторное криптографическое техническое средство аутентификации
		Усиленная аутентификация[1)]	Многофакторный генератор одноразовых паролей (техническое устройство или программа)
		Строгая аутентификация[2)]	Многофакторное криптографическое программное средство аутентификации, многофакторное криптографическое техническое средство аутентификации, многофакторное криптографическое техническое средство аутентификации с неизвлекаемым ключом
Средний уровень доверия аутентификации	Умеренная уверенность в том, что субъект доступа, успешно прошедший идентификацию и аутентификацию, действительно является тем зарегистрированным субъектом доступа, за которого себя выдает предъявленным идентификатором доступа при условии, что субъект доступа имеет и контролирует аутентификатор	Усиленная аутентификация	Многофакторный генератор одноразовых паролей (техническое устройство или программа) или запоминаемый секрет, используемый совместно с поисковым секретом, или внеполосным секретом, или однофакторным генератором одноразовых паролей
		Строгая аутентификация[3)]	Многофакторное криптографическое программное средство, многофакторное криптографическое техническое средство аутентификации, многофакторное криптографическое техническое средство аутентификации с неизвлекаемым ключом или запоминаемый секрет, используемый совместно с однофакторным криптографическим программным средством аутентификации, или однофакторным криптографическим техническим средством аутентификации
Высокий уровень доверия аутентификации	Значительная уверенность в том, что и субъект доступа, успешно прошедший идентификацию и аутентификацию, и объект доступа, успешно прошедший аутентификацию, действительно являются теми зарегистрированными субъектом и объектом доступа, за которого себя выдает каждый из них при условии, что субъект (объект) доступа имеет	Строгая аутентификация	Многофакторное криптографическое техническое средство аутентификации, или однофакторное криптографическое техническое средство аутентификации совместно с запоминаемым секретом, или многофакторный генератор одноразовых паролей (техническое устройство или программа) совместно с однофакторным криптографическим техническим средством аутентификации,

Окончание таблицы А.1

Уровень доверия аутентификации	Уверенность в результатах аутентификации	Виды аутентификации	Средства аутентификации
Высокий уровень доверия аутентификации	и контролирует аутентификатор, который используется в криптографических средствах аутентификации, реализующих применение не менее двух различных факторов при аутентификации	Строгая аутентификация	или многофакторный генератор одноразовых паролей (техническое устройство) совместно с однофакторным криптографическим программным средством аутентификации, или однофакторный генератор одноразовых паролей (техническое устройство) совместно с многофакторным криптографическим программным средством аутентификации, или однофакторный генератор одноразовых паролей (техническое устройство) совместно с однофакторным криптографическим программным средством аутентификации и запоминаемым секретом
	Максимальная уверенность в том, что и субъект доступа, успешно прошедший идентификацию и аутентификацию, и объект доступа, успешно прошедший аутентификацию, действительно являются теми зарегистрированными субъектом и объектом доступа, за которого себя выдает каждый из них при условии, что субъект (объект) доступа имеет и контролирует аутентификатор, который используется в криптографических технических средствах аутентификации с неизвлекаемыми ключами, реализующих применение не менее двух различных факторов при аутентификации		Многофакторное криптографическое техническое средство аутентификации с неизвлекаемыми ключами

[1] Усиленная аутентификация может использоваться по решению оператора в конкретной среде функционирования для обеспечения низкого уровня доверия.

[2] Строгая аутентификация может использоваться по решению оператора в конкретной среде функционирования для обеспечения низкого уровня доверия.

[3] Строгая аутентификация может использоваться по решению оператора в конкретной среде функционирования для обеспечения среднего уровня доверия.

Библиография

[1] ИСО/МЭК 29115:2013 Информационная технология. Методы и средства обеспечения безопасности. Основы доверия аутентификации сущности (Information technology — Security techniques — Entity authentication assurance framework)

[2] ITU-T Rec. X.811 (04/95) Информационная технология. Взаимосвязь открытых систем. Основы безопасности для открытых систем. Основы аутентификации (Information technology — Open Systems Interconnection — Security frameworks for open systems: Authentication framework)

[3] NIST SP 800-63B Руководства по цифровым идентичностям. Аутентификация и менеджмент жизненного цикла (Digital Identity Guidelines: Authentication and Lifecycle Management)

[4] RFC 4120 Сетевая служба аутентификации Kerberos версии 5 (The Kerberos Network Authentication Service V5)

[5] ITU-T Rec. X.509 (10/19) Информационная технология. Взаимосвязь открытых систем. Справочник. Структура сертификатов открытых ключей и сертификатов атрибутов (Information technology — Open Systems Interconnection — The Directory: Public-key and attribute certificate frameworks)

[6] Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»

[7] Р 50.1.053—2005 Информационные технологии. Основные термины и определения в области технической защиты информации

[8] Р 50.1.056—2005 Техническая защита информации. Основные термины и определения

УДК 004:006.354 ОКС 35.030

Ключевые слова: защита информации, аутентификация, управление доступом, аутентификационная информация, аутентификатор, аутентификационный обмен, виды аутентификации, средства аутентификации, уровень доверия аутентификации

Редактор *М.В. Митрофанова*
Технический редактор *В.Н. Прусакова*
Корректор *И.А. Королева*
Компьютерная верстка *И.А. Налейкиной*

Сдано в набор 02.06.2025. Подписано в печать 05.06.2025. Формат 60×84⅛. Гарнитура Ариал.
Усл. печ. л. 3,26. Уч.-изд. л. 2,64.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

Создано в единичном исполнении в ФГБУ «Институт стандартизации»
для комплектования Федерального информационного фонда стандартов,
117418 Москва, Нахимовский пр-т, д. 31, к. 2.
gost.e-ecolog.ru gost.e-ecolog.ru