ФЕДЕРАЛЬНОЕ АГЕНСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р

(проект, окончательная редакция)

Защита информации

ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ

Общие положения

Настоящий проект стандарта не подлежит применению до его утверждения

20XX

ГОСТ Р
(проект, окончательная редакция)

Предисловие

1 РАЗРАБОТАН Федеральной службой по техническому и экспортному контролю (ФСТЭК России), Закрытым акционерным обществом «Аладдин Р.Д.» (ЗАО «Аладдин Р.Д.») и Обществом с ограниченной ответственностью «Научно-производственная фирма «КРИСТАЛЛ» (ООО «НПФ «КРИСТАЛЛ»)

2 ВНЕСЕН Техническим комитетом по стандартизации «Защита информации» (ТК 362) и Техническим комитетом по стандартизации «Криптографическая защита информации» (ТК 26).

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ приказом Федерального агентства по техническому регулированию и метрологии от «___» _____ 20__ № _____

4 ВВЕДЕН ВПЕРВЫЕ

Правила применения настоящего стандарта установлены в статье 26 Федерального закона «О стандартизации в Российской Федерации». Информация об изменениях к настоящему стандарту публикуется в годовом (по состоянию на 1 января текущего года) информационном указателе «Национальные стандарты», а официальный текст изменений и поправок – в ежемесячно издаваемом 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 органа исполнительной власти в сфере стандартизации в сети

Интернет (www.gost.ru).

Содержание

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.

При автоматизированной обработке информации физическому лицу, как субъекту доступа, соответствуют вычислительные процессы, выполняющие операции с данными. Это создает риски неоднозначного сопоставления вычислительных процессов с конкретным физическим лицом. Аналогичные риски существуют и при автоматической обработке информации. Кроме того, удаленное информационное взаимодействие дополнительно порождает риск ошибочной идентификации удаленного субъекта доступа и, следовательно, риск предоставления доступа злоумышленнику. Наряду с этим существуют риски того, что вычислительный процесс, действующий в интересах злоумышленника, может имитировать объекты (субъекты) доступа, функционирующие как параллельно с легальными, так и существующие независимо от них.

Устанавливая правила управления доступом к информации и сервисам, обеспечивающим ее обработку, для различных категорий субъектов доступа, необходимо учитывать не только конфиденциальность защищаемой информации, но и указанные риски. Для снижения рисков должны применяться соответствующие методы идентификации и аутентификации, которые обеспечат уверенность в подлинности сторон, участвующих в информационном взаимодействии, включая и субъекты доступа, и объекты доступа. Это особенно востребовано в том случае, когда

взаимодействующие стороны имеют дефицит взаимного доверия, обусловленный, например, использованием небезопасной среды функционирования.

Для понимания положений настоящего стандарта необходимы знания основ информационных технологий, а также способов защиты информации.

ГОСТ Р
(проект, окончательная редакция)

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Защита информации

ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ

Общие положения

Information protection. Identification and authentication. General

Дата введения — _____

1 Область применения

Настоящий стандарт устанавливает единообразную организацию процессов идентификации и аутентификации в средствах защиты информации, в том числе реализующих криптографическую защиту, средствах вычислительной техники и автоматизированных (информационных) системах, а также определяет общие правила применения методов идентификации и аутентификации, обеспечивающих необходимую уверенность в результатах.

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

Настоящий стандарт определяет состав участников и основное содержание процессов идентификации и аутентификации, рекомендуемое к реализации при разработке, внедрении и совершенствовании правил, механизмов и технологий управления доступом. 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.

Настоящий стандарт предназначен для применения путем включения нормативных ссылок на него в соответствии с действующим законодательством и (или) прямого использования устанавливаемых в нем положений.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

ГОСТ Р 50922–2006 Защита информации. Основные термины и определения

ГОСТ Р 56939–2016 Защита информации. Разработка безопасного программного обеспечения. Общие требования

ГОСТ Р ИСО/МЭК 27005–2010 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 указателю «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 50922–2006, а также следующие термины с соответствующими определениями:

3.1 **анонимный субъект доступа, «аноним»**: **Субъект доступа** (3.55), **первичная идентификация** (3.41) которого выполнена в конкретной **среде функционирования** (3.53), но при этом его **идентификационные данные** (3.22) не соответствуют требованиям к **первичной идентификации** (3.41) или не подтверждались.

3.2 **атрибут**: Признак или свойство **субъекта доступа** (3.55) или **объекта доступа** (3.33).

3.3 **аутентификационная информация**: Информация, используемая при **аутентификации** (3.4) **субъекта доступа** (3.55) или **объекта доступа** (3.33).

3.4 **аутентификация**: Действия по проверке **подлинности** (3.42) **субъекта доступа** (3.55) и/или **объекта доступа** (3.33), а также по проверке принадлежности **субъекту доступа** (3.55) и/или **объекту доступа**

(3.33) предъявленного **идентификатора доступа** (3.20) и **аутентификационной информации** (3.3).

Примечания

1 Адаптировано из Р 50.1.053-2005.

2 **Аутентификация** (3.4) рассматривается применительно к конкретному **субъекту доступа** (3.55) и/или конкретному **объекту доступа** (3.33).

3.5 **аутентификация анонимного субъекта доступа, анонимная аутентификация**: Аутентификация, используемая для подтверждения **подлинности** (3.42) **анонимного субъекта доступа** (3.1).

3.6 **биометрические данные:** Сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность [1].

3.7 **верификатор идентификации**: **Доверенный объект** (3.14), выполняющий **вторичную идентификацию** (3.12) **субъекта доступа** (3.55) при доступе.

3.8 **верификатор аутентификации**: **Доверенный объект** (3.14), выполняющий **аутентификацию** (3.4) **субъекта доступа** (3.55) при доступе.

3.9 **верификация**: **Процесс** (3.48) проверки информации путем сопоставления предоставленной информации с ранее подтвержденной информацией.

3.10 **взаимная аутентификация**: Обоюдная аутентификация, обеспечивающая для каждого из участников **процесса** (3.48) **аутентификации** (3.4), и **субъекту доступа** (3.55), и **объекту доступа** (3.33), **уверенность** (3.56) в том, что другой участник **процесса** (3.48) **аутентификации** (3.4) является тем, за кого себя выдаёт.

3.11

виртуальный (virtual): Определение, характеризующее процесс или устройство в системе обработки информации кажущихся реально су-

ществующими, поскольку все их функции реализуются какими-либо другими средствами.

[ГОСТ 33707—2016 Информационные технологии. Словарь, пункт 4.151]

3.12 **вторичная идентификация**: Действия по проверке существования (наличия) **идентификатора** (3.20), предъявленного **субъектом доступа** (3.55) при **доступе** (3.17), в перечне **идентификаторов доступа** (3.20), которые были присвоены **субъектам доступа** (3.55) и **объектам доступа** (3.33) при **первичной идентификации** (3.41).

Примечание – **Вторичная идентификация** (3.12) рассматривается применительно к конкретному **субъекту доступа** (3.55).

3.13

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]

3.14 **доверенный объект**: объект, который будет действовать в полном соответствии с ожиданиями и **субъекта доступа** (3.55) и **объекта доступа** (3.33) или любого их них, при этом выполняя то, что он должен делать и не выполняя то, что он не должен делать [2].

3.15 **доверенная третья сторона:** Участник **процесса** (3.48) **аутентификации** (3.4), предоставляющий один или более сервисов в области защиты информации, которому доверяют другие участники **процесса** (3.48) **аутентификации** (3.4) как поставщику данных услуг.

Примечания

1 При **аутентификации** (3.4) **доверенной третьей стороне** (3.15) доверяют и **субъект доступа** (3.55) и **объект доступа** (3.33).

2 В качестве **доверенной третьей стороны** (3.15) могут рассматриваться: организация (например, осуществляющая функции удостоверяющего центра), администратор автоматизированной (информационной) системы, устройство.

3 **Доверенная третья сторона** (3.15) является **доверенным объектом** (3.14).

3.16

доверие (assurance): Выполнение соответствующих действий или процедур для обеспечения уверенности в том, что оцениваемый объект соответствует своим целям безопасности.

ГОСТ Р 54581-2011/ISO/IEC/TR 15443-1:2005, пункт 2.4.

Примечание – Результаты, получаемые в рамках обеспечения **доверия** (3.16) рассматриваются в качестве оснований для **уверенности** (3.56).

3.17 **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** (3.25), **вычислительные ресурсы** (3.13) средств вычислительной техники и **ресурсы автоматизированных (информационных) систем** (3.49), а также средства вычислительной техники и автоматизированные (информационные) системы в целом.

2 Доступ к информации - возможность получения информации и ее использования [3].

3.18 **закрытый ключ:** Ключ из состава асимметричной пары ключей, сформированных для объекта, который должен быть использован только этим объектом [4].

Примечания

1 Закрытый ключ не является общедоступным [4].

2 Ключ электронной подписи [5] является примером закрытого ключа.

3.19 **закрытый ключ неизвлекаемый: Закрытый ключ** (3.18), который при его формировании и хранении невозможно извлечь из **устройства аутентификации** (3.60), в котором он был создан.

Примечание – Неизвлекаемость **закрытого ключа** (3.18) заключается в от-

сутствии возможности его извлечения из **устройства аутентификации** (3.60), в котором он был создан, штатными средствами, предоставляемыми данным **устройством аутентификации** (3.60). Неизвлекаемость **закрытого ключа** (3.18) в **устройствах аутентификации** (3.60), как правило, обеспечивается применяемыми схемотехническими решениями и гарантируется производителями устройств.

3.20 **идентификатор доступа (субъекта (объекта) доступа), идентификатор**: Признак **субъекта доступа** (3.55) или **объекта доступа** (3.33) в виде строки знаков (символов), который используется при **идентификации** (3.24) и однозначно определяет (указывает) соотнесенную с ними **идентификационную информацию** (3.21).

3.21 **идентификационная информация**: Совокупность значений **идентификационных атрибутов** (3.23), которая связана с конкретным **субъектом доступа** (3.55) или конкретным **объектом доступа** (3.33).

3.22 **идентификационные данные**: Совокупность **идентификационных атрибутов** (3.23) и их значений, которая связана с конкретным **субъектом доступа** (3.55) или конкретным **объектом доступа** (3.33).

3.23 **идентификационный атрибут**: Атрибут, который характеризует **субъект доступа** (3.55) или **объект доступа** (3.33) и может быть использован для его распознавания.

3.24

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

[Р 50.1.053-2005, пункт 3.3.9]

3.25

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, раздел 2, пункт 11]

3.26 **ключ:** Изменяемый параметр в виде последовательности символов, определяющий криптографическое преобразование [6].

3.27 **метод аутентификации**: Реализуемое при **аутентификации** (3.4) предопределенное сочетание **факторов аутентификации** (3.61), организации обмена и обработки **аутентификационной информации** (3.3), а также соответствующих данному сочетанию **протоколов аутентификации** (3.47).

3.28

метод обеспечения доверия: Общепризнанная спецификация получения воспроизводимых результатов обеспечения доверия.

[ГОСТ Р 54581-2011/ISO/IEC/TR 15443-1:2005, пункт 2.11]

3.29 **многофакторная аутентификация**: **Аутентификация** (3.4), при выполнении которой используется не менее двух различных **факторов аутентификации** (3.61).

3.30 **многошаговая идентификация и аутентификация**: **Идентификация** (3.24) и **аутентификация** (3.4), осуществляемая при **доступе** (3.17) **субъекта доступа** (3.55) к **объекту доступа** (3.33) и состоящая из последовательности **процессов** (3.48) («шагов») **идентификации** (3.24) и **аутентификации** (3.4).

Примечания

1 В рамках последовательности **процессов** (3.48) («шагов») **идентификации** (3.24) и **аутентификации** (3.4) осуществляется **вторичная идентификация** (3.12) **субъекта доступа** (3.55).

2 В рамках последовательности **процессов** (3.47) («шагов») **идентификации** (3.24) и **аутентификации** (3.4) могут использоваться различные или одинаковые виды аутентификации: **простая аутентификация** (3.46), **усиленная аутентификация** (3.59), **строгая аутентификация** (3.54).

3.31 **несанкционированный доступ**: **Доступ** (3.17) **субъекта доступа** (3.55) **к объекту доступа** (3.33), нарушающий **правила управления доступом** (3.45).

Примечание – Адаптировано из Р 50.1.056-2005.

3.32 **обладатель информации**: лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам [3].

3.33 **объект доступа**: Одна из сторон информационного взаимодействия, которая предоставляет **доступ** (3.17).

3.34 **объективное свидетельство**: Данные, подтверждающие наличие или истинность чего-либо.

Примечания

1 Объективное свидетельство может быть получено путем наблюдения, измерения, испытания или другим способом.

2 Адаптировано из ГОСТ Р ИСО 9000-2015.

3.35 **одноразовый пароль**: Однократно используемый **пароль** (3.40).

Примечание – Возможность использования для аутентификации **одноразового пароля** (3.35) прекращается (исключается) при наступлении события получения **доступа** (3.17) **субъектом доступа** (3.55) или события отказа **субъектом доступа** (3.55) от получения **доступа** (3.17) или события отказа **объектом доступа** (3.33) в предоставлении **доступа** (3.17).

3.36 **односторонняя аутентификация**: **Аутентификация** (3.4), обеспечивающая только лишь для одного из участников **процесса** (3.47) **аутентификации** (3.4) – **объекта доступа** (3.33) – уверенность в том, что другой участник **процесса** (3.48) **аутентификации** (3.4) – **субъект доступа** (3.55) – является тем, за кого себя выдаёт предъявленным **идентификатором доступа** (3.20).

3.37 **однофакторная аутентификация**: **Аутентификация** (3.4), при выполнении которой используется один **фактор аутентификации** (3.61).

3.38 **оператор автоматизированной (информационной) системы, оператор:** физическое или юридическое лицо, осуществляющие

деятельность по эксплуатации автоматизированной (информационной) системы, в том числе по обработке информации, содержащейся в ее базах данных [3].

3.39 **открытый ключ:** Ключ, из состава асимметричной пары ключей, сформированных для объекта, который может быть общедоступным [4].

Примечание – Ключ проверки электронной подписи [5] является примером открытого ключа.

3.40

пароль: Конфиденциальная аутентификационная информация, обычно состоящая из строки знаков.

[ГОСТ Р ИСО 7498-2–99, пункт 3.3.39]

3.41 **первичная идентификация**: Действия по формированию и регистрации информации о **субъекте доступа** (3.55) или **объекте доступа** (3.33), а также действия по присвоению **идентификатора доступа** (3.20) **субъекту доступа** (3.55) или **объекту доступа** (3.33) и его регистрации в перечне присвоенных **идентификаторов доступа** (3.20).

Примечание – **Первичная идентификация** (3.41) рассматривается применительно к конкретному **субъекту доступа** (3.55) и/или конкретному **объекту доступа** (3.33).

3.42

подлинность (authenticity): Свойство, гарантирующее, что субъект или ресурс идентичен заявленному.

[ГОСТ Р ИСО/МЭК 27000-2012, пункт 2.6]

3.43 **подтверждающая информация**: Информация, собранная и использованная для подтверждения **идентификационных данных** (3.22) в соответствии с установленными требованиям к **первичной идентификации** (3.40).

3.44 **пользователь**: Физическое лицо, **первичная идентификация** (3.41) которого выполнена в конкретной **среде функционирования**

(3.53).

Примечание – Например, **пользователем** (3.43) автоматизированной (информационной) системы, является физическое лицо, **первичная идентификация** (3.41) которого выполнена в конкретной автоматизированной (информационной) системе. После успешной **вторичной идентификации** (3.12) и **аутентификации** (3.4) **пользователь** (3.44) (вычислительный **процесс** (3.48) от его имени) получает **доступ** (3.17) к **ресурсам автоматизированной (информационной) системы** (3.49) для их использования.

3.45 **правила управления доступом**: Правила, регламентирующие условия **доступа** (3.17) **субъектов доступа** (3.55) к **объектам доступа** (3.33) на основе прав доступа.

Примечания

1 Адаптировано из Р 50.1.053-2005.

2 Права доступа определяют набор действий, которые **субъекты доступа** (3.55) могут выполнять над **объектами доступа** (3.33) в конкретной **среде функционирования** (3.53).

3 Условия доступа определяют перечень разрешенных (запрещенных) действий **субъектов доступа** (3.55) над **объектами доступа** (3.33) в конкретной **среде функционирования** (3.53).

4 **Правила управления доступом** (3.45) могут устанавливаться нормативными правовыми документами, **обладателем информации** (3.32) или **оператором** (3.38).

3.46 **простая аутентификация: Аутентификация** (3.4) с применением метода **однофакторной** (3.37) **односторонней** (3.36) **аутентификации** (3.4) и соответствующих данному методу **протоколов аутентификации** (3.47).

3.47 **протокол аутентификации:** Протокол, позволяющий участникам **процесса** (3.48) **аутентификации** (3.4), осуществить **аутентификацию** (3.4).

Примечание – Протокол реализует алгоритм (правила), в рамках которого **субъект доступа** (3.55) и **объект доступа** (3.33) последовательно выполняют определенные действия и обмениваются сообщениями.

3.48

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

[ГОСТ Р ИСО 9000-2015, пункт 3.4.1]

3.49

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

[Р 50.1.056-2005, пункт А.20]

3.50 **санкционирование доступа, авторизация**: Предоставление **субъекту доступа** (3.55) прав **доступа** (3.17), а также предоставление **доступа** (3.17) в соответствии с установленными **правилами управления доступом** (3.45).

Примечания

1 Адаптировано из Р 50.1.056-2005.

2 Положительный результат **идентификации** (3.24) и **аутентификации** (3.4) является одним из оснований для **авторизации** (3.50) субъекта доступа (3.55).

3.51 **санкционированный доступ**: **Доступ** (3.17) **субъекта доступа** (3.55) к **объекту доступа** (3.33), не нарушающий **правила управления доступом** (3.45).

3.52 **свидетельство идентичности, свидетельство: Объективное свидетельство** (3.34), обеспечивающее **уверенность** (3.56) в том, что **идентификационные данные** (3.22) действительно соответствуют (принадлежат) **субъекту доступа** (3.55) или **объекту доступа** (3.33), который их заявил.

Примечание – В качестве **свидетельств идентичности** (3.52) могут рассматриваться, например, результаты **верификации** (3.9) заявленных **идентификационных данных** (3.22), документальные подтверждения (официальные документы),

представленные **субъектом доступа** (3.55), а также другая **подтверждающая информация** (3.43).

3.53 **среда функционирования**: Среда с предопределенными (установленными) граничными условиями, в которой существуют (функционируют) и взаимодействуют **субъекты доступа** (3.55) и **объекты доступа** (3.33).

Примечания

1 Область действия **правил управления доступом** (3.45) рассматривается как граничное условие **среды функционирования** (3.53).

2 Граничные условия **среды функционирования** (3.53) могут определяться, например, нормативными и правовыми документами, обладателем информации или **оператором** (3.37).

3.54 **строгая аутентификация: Аутентификация** (3.4) с применением только метода **многофакторной** (3.29) **взаимной** (3.10) **аутентификации** (3.4) и использованием криптографических **протоколов аутентификации** (3.47).

3.55 **субъект доступа**: Одна из сторон информационного взаимодействия, которая инициирует получение и получает **доступ** (3.17).

Примечание – **Субъектами доступа** (3.55) могут являться как физические лица (**пользователи** (3.44)), так и ресурсы стороны информационного взаимодействия, а также вычислительные **процессы** (3.48), инициирующие получение и получающие **доступ** (3.17) от их имени.

3.56

уверенность (confidence): 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/ISO/IEC/TR 15443-1:2005, пункт 2.18.

3.57 **управление доступом**: Предоставление **санкционированного** (3.50) и предотвращение **несанкционированного** (3.31) **доступа** (3.17).

Примечание – Адаптировано из ГОСТ Р ИСО/МЭК ТО 10032-2007.

3.58

уровень доверия (assurance level): Степень доверия, соответствующая специальной шкале, применяемой в методе обеспечения доверия.

Примечания

1 Уровень доверия не измеряется количественными показателями.

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

[ГОСТ Р 54581-2011/ISO/IEC/TR 15443-1:2005, пункт 2.10]

3.59 **усиленная аутентификация: Аутентификация** (3.4) с применением метода **многофакторной** (3.29) **односторонней** (3.36) или **взаимной** (3.10) **аутентификации** (3.4) и соответствующих данному методу **протоколов аутентификации** (3.47).

3.60 **устройство аутентификации**: Техническое (аппаратное) или **виртуальное** (3.11) устройство, содержащее информацию о его обладателе, которая может использоваться при **идентификации** (3.24) и/или **аутентификации** (3.4).

Примечание – Адаптировано из ГОСТ Р ИСО/МЭК 24713-2-2011.

3.61 **фактор аутентификации**: Вид (форма) существования **аутентификационной информации** (3.3), предъявляемой **субъектом доступа** (3.55) или **объектом доступа** (3.33) при **аутентификации** (3.4).

3.62 **электронное удостоверение:** Совокупность **идентификационной информации** (3.21) и **аутентификационной информации** (3.3) (или прямого указания ее существования) **субъекта доступа** (3.55) или **объекта доступа** (3.33), **подлинность** (3.42) которой подтверждена **доверенной третьей стороной** (3.15).

Примечания

1 **Электронное удостоверение** (3.62) может выпускаться **доверенной третьей стороной** (3.15) с возможностью проверки его действительности [7] на момент предоставления **доступа** (3.17) конкретному **субъекту доступа** (3.55) к конкретному

объекту доступа (3.33).

2 **Электронное удостоверение** (3.62) может представлять собой: в простейшем случае **идентификатор доступа** (3.20) и **пароль** (3.40); в других случаях – совокупность **идентификатора доступа** (3.20), **открытого ключа** (3.39) и другой информации.

3 Порядок и правила формирования и применения **электронных удостоверений** (3.62) определяются соответствующими действующими нормативными правовыми документами и документами по стандартизации.

Взаимосвязь терминов, которые входят в группы, относящиеся к понятиям «идентификация» и «аутентификация», и ее графическое представление приведены в приложении А.

4 Сокращения

В настоящем стандарте применены следующие сокращения:

PIN (Personal Identification Number) – персональный идентификационный номер.

5 Общие положения

5.1 Целью идентификации и аутентификации при доступе субъекта доступа к объекту доступа является распознавание субъекта доступа с необходимой уверенностью в том, что он является именно тем, за кого

себя выдает. При этом степень достижения цели идентификации и аутентификации определяется уровнем доверия к результатам идентификации и аутентификации.

5.2 В общем случае идентификация и аутентификация охватывают:

- первичную идентификацию, включающую формирование и регистрацию информации о субъекте (объекте) доступа, а также присвоение субъекту (объекту) доступа идентификатора доступа и его регистрацию в перечне присвоенных идентификаторов;

- хранение и поддержание актуального состояния (обновление) идентификационной и аутентификационной информации субъекта (объекта) доступа в соответствии с установленными правилами;

- вторичную идентификацию, которая обеспечивает опознавание субъекта доступа, запросившего доступ к объекту доступа, по предъявленному идентификатору;

- аутентификацию, включающую проверку подлинности субъекта (объекта) доступа и принадлежности ему предъявленных идентификатора и аутентификационной информации.

Примечание – Применительно к объекту доступа проверка подлинности осуществляется при взаимной аутентификации.

5.3 Идентификация и аутентификация осуществляются в области действия единых правил управления доступом.

Примечания

1 Правила управления доступом (единые правила управления доступом) могут быть реализованы, например, в границах: одного или нескольких вычислительных процессов; одного или нескольких средств вычислительной техники; одной или нескольких автоматизированных (информационных) систем.

2 Идентификация и аутентификация могут осуществляться, например, в границах одной автоматизированной (информационной) системы (области действия правил управления доступом); в границах нескольких автоматизированных (информационных) систем, находящихся под управлением одного оператора, при условии распространения на них единых правил управления доступом, или в границах нескольких

автоматизированных (информационных) систем, находящихся под управлением различных операторов, при условии согласования правил управления доступом операторами данных автоматизированных (информационных) систем.

3 Для идентификации и аутентификации могут использоваться внешние по отношению к области действия единых правил управления доступом сервисы, предоставляемые, например, доверенной третьей стороной.

5.4 При доступе к объекту доступа идентификация и аутентификация субъекта доступа может осуществляться как в рамках одного процесса идентификации и аутентификации, так и выполняться в рамках последовательности процессов идентификации и аутентификации (многошаговая идентификация и аутентификация).

Примечания

1 При многошаговой идентификации и аутентификации после положительного результата проверки идентификатора доступа и аутентификационной информации на одном «шаге» предоставляется доступ к проверке идентификатора доступа и аутентификационной информации следующего «шага». Результат проверки на каждом «шаге» доводится субъекту доступа, а после положительного результата проверки на последнем «шаге» предоставляется доступ к объекту доступа. При отрицательном результате проверки на любом из «шагов» дальнейшая последовательность процессов идентификации и аутентификации не выполняется.

2 При многошаговой идентификации и аутентификации для проверки идентификатора доступа и аутентификационной информации в рамках последовательно осуществляемых процессов идентификации и аутентификации («шагов») могут использоваться различные устройства, средства вычислительной техники и/или автоматизированные (информационные) системы, а также сервисы, внешние по отношению к участникам идентификации и аутентификации.

5.5 При доступе участники процессов идентификации и аутентификации имеют следующее функциональное назначение (функциональные роли):

- сторона, инициирующая доступ. Основной задачей стороны, инициирующей доступ, является запрос доступа и последующее предоставление информации, необходимой другим сторонам;

- регистрирующая сторона. Основной задачей регистрирующей стороны является присвоение субъекту (объекту) доступа идентификатора доступа и, при необходимости, аутентификационной информации, их регистрация и поддержание в актуальном состоянии (обновление), а также фиксация связи идентификатора и аутентификационной информации с конкретным субъектом (объектом) доступа;

- доверяющая сторона. Основной задачей доверяющей стороны является опознавание субъекта доступа по предъявленному идентификатору и проверка его подлинности;

- проверяющая сторона. Основной задачей проверяющей стороны является проверка принадлежности субъекту доступа идентификатора доступа и аутентификационной информации, которая зафиксированы за ним регистрирующей стороной.

5.6 Отдельные функциональные роли могут быть объединены и/или назначены участникам процессов идентификации и аутентификации.

Примечание – Доверенная третья сторона, например, может объединять (выполнять) функциональные роли регистрирующей и проверяющей сторон, объект доступа – функциональные роли регистрирующей, проверяющей и доверяющей сторон, а субъект доступа – функциональные роли стороны, инициирующей доступ, проверяющей и доверяющей сторон (при взаимной аутентификации).

6 Основы идентификации

6.1 Процесс идентификации должен включать действия по формированию идентификационной информации субъекта (объекта) доступа, присвоению субъекту (объекту) доступа идентификатора и их последующей регистрации, а при доступе субъекта доступа к объекту доступа –

действия по проверке существования (наличия) идентификатора, предъявленного субъектом доступа, в перечне присвоенных идентификаторов.

6.2 Идентификация разделяется на первичную идентификацию, осуществляемую при регистрации регистрирующей стороной нового субъекта (объекта) доступа, и вторичную идентификацию, регулярно повторяющуюся при каждом запросе субъекта доступа на доступ.

Для поддержания актуального состояния (обновления) идентификационной информации зарегистрированного субъекта (объекта) доступа первичная идентификация может повторяться с установленной периодичностью или по мере необходимости, а также выполняться по запросу субъекта (объекта) доступа. Вторичная идентификация субъекта доступа может выполняться однократно или, при необходимости, с установленной периодичностью в течение всего информационного взаимодействия между субъектом доступа и объектом доступа.

Общая характеристика типового процесса идентификации приведена в Приложении Б.

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

6.4 До первичной идентификации регистрирующей стороной должны быть установлены требования к первичной идентификации, которые определяют объем, состав и обязательность идентификационных атрибутов субъекта (объекта) доступа, используемых для формирования идентификационной информации, а также устанавливают необходимость, порядок и правила подтверждения заявленных субъектом (объектом) доступа идентификационных данных.

В конкретной среде функционирования каждый субъект (объект) доступа должен иметь единственный набор значений идентификационных

атрибутов, связанный с идентификатором доступа, что обеспечит однозначную идентификацию данного субъекта (объекта) доступа.

6.5 При первичной идентификации регистрирующей стороне необходимо оценить идентификационные данные, заявленные субъектом (объектом) доступа, на соответствие установленным требованиями, а также установить и подтвердить соответствие между субъектом доступа и его идентификационными данными. Для этого:

- при оценке заявленных идентификационных данных, как минимум, надлежит проверить наличие у регистрирующей стороны идентификационной информации, связанной с субъектом (объектом) доступа, ее уникальность и актуальность, а также определить – достаточно ли предъявлено идентификационных атрибутов для однозначной идентификации субъекта (объекта) доступа;

- при подтверждении заявленных идентификационных данных, как минимум, надлежит проверить их существование путем верификации и получения свидетельств, а также установить связь (осуществить привязку) между субъектом (объектом) доступа и заявленными идентификационными данными;

Примечания

1 При верификации регистрирующая сторона может использовать собственную подтверждающую информацию, подтверждающую информацию, которая предоставлена субъектом (объектом) доступа, а также может использовать внешние (по отношению к регистрирующей стороне) сервисы, предоставляемые, например, доверенной третьей стороной.

2 Свидетельства являются результатом верификации заявленных идентификационных данных с использованием, как правило (но не только), внешних сервисов, в том числе имеющих возможность официального подтверждения идентификационных данных.

6.6 По результатам первичной идентификации субъекту (объекту) доступа должен присваиваться уникальный идентификатор доступа,

определяющий соотнесенную с ним идентификационную информацию субъекта (объекта) доступа. Уникальность идентификатора доступа должна обеспечиваться в области действия единых правил управления доступом.

Идентификатор доступа может назначаться субъекту (объекту) доступа регистрирующей стороной или самостоятельно создаваться субъектом доступа в соответствии с установленными правилами.

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

6.8 Первичная идентификация субъекта (объекта) доступа должна завершаться регистрацией идентификационной информации и присвоенного субъекту (объекту) доступа уникального идентификатора доступа или обоснованным отказом. Основанием для отказа в регистрации может быть несоответствие заявленных идентификационных данных требованиям к первичной идентификации или невозможность их подтверждения в установленном порядке.

Примечание – В качестве оснований для отказа, например, могут рассматриваться недостаточный объем идентификационных данных, представленных субъектом (объектом) доступа, отрицательный результат их верификации или отсутствие необходимой подтверждающей информации.

По решению регистрирующей стороны возможна регистрация субъекта доступа, идентификационные данные которого не соответствуют требованиям к первичной идентификации или не были подтверждены. При этом субъекту доступа присваивается уникальный идентификатор,

субъект доступа определяется как анонимный субъект доступа («аноним») и нет никакой уверенности том, что заявленные идентификационные данные действительно соответствуют (принадлежат) данному субъекту доступа.

6.9 Первичная идентификация должна являться неотъемлемой частью как процесса идентификации, не предусматривающего аутентификацию и последующий доступ субъекта доступа, так и частью процесса идентификации, предполагающего последующий доступ субъекта доступа и, соответственно, его аутентификацию.

Примечание – Примером первичной идентификации, не предусматривающей последующий доступ, может считаться внесение идентификационной информации физических лиц в автоматизированную (информационную) систему, которая используются для предоставления данной идентификационной информации другим автоматизированным (информационным) системам. Физические лица не являются пользователями данной автоматизированной (информационной) системы.

6.10 Целью вторичной идентификации является опознавание субъекта доступа, запросившего доступ к объекту доступа. При этом должна выполняться проверка существования идентификатора доступа, предъявленного субъектом доступа, в перечне присвоенных идентификаторов. При наличии предъявленного идентификатора доступа в перечне присвоенных идентификаторов процесс вторичной идентификации должен считаться успешно пройденным.

Примечание – Проверка существования (наличия) идентификатора доступа, предъявленного субъектом доступа, в перечне присвоенных идентификаторов, осуществляется по предопределенному алгоритму и может выполняться, в том числе, путем сравнения.

6.11 Процесс идентификации, не предусматривающий последующий доступ, в общем виде должен включать:

- представление физическим лицом или получение от ресурса идентификационных данных, необходимых для первичной идентификации;

- оценка возможности регистрации идентификационной информации регистрирующей стороной и подтверждение соответствия между физическим лицом (ресурсом) и его идентификационными данными;

- принятие регистрирующей стороной решения о результате первичной идентификации, в том числе регистрация идентификационной информации и присвоенного физическому лицу (ресурсу) идентификатора, или обоснованный отказ в регистрации;

- хранение и поддержание идентификационной информации в актуальном состоянии (обновление) регистрирующей стороной и, при необходимости, предоставление ее по запросам.

6.12 Процесс идентификации, предусматривающий последующие аутентификацию, авторизацию и доступ, в общем виде должен включать:

- формирование запроса на регистрацию субъекта (объекта) доступа и последующее представление идентификационных данных, необходимых для первичной идентификации;

- оценка регистрирующей стороной возможности регистрации идентификационной информации и подтверждение соответствия между субъектом (объектом) доступа и его идентификационными данными;

- принятие регистрирующей стороной решения о результате первичной идентификации, в том числе регистрация идентификационной информации и присвоенного субъекту (объекту) доступа идентификатора доступа или обоснованный отказ в регистрации;

- хранение и поддержание в актуальном состоянии (обновление) идентификатора доступа и идентификационной информации регистрирующей стороной;

- предъявление доверяющей стороне субъектом доступа идентификатора для вторичной идентификации при запросе доступа к объекту доступа;

- проверка доверяющей стороной существования (наличия) идентификатора, предъявленного субъектом доступа, в перечне присвоенных идентификаторов;

- контроль проверяющей стороной принадлежности субъекту доступа идентификатора доступа, включая проверку актуальности (действительности) и проверку связи идентификатора доступа с субъектом доступа;

- принятие решения доверяющей стороной о результате вторичной идентификации и последующем проведении аутентификации.

7 Основы аутентификации

7.1 Процесс аутентификации при доступе субъекта доступа к объекту доступа должен включать действия по проверке подлинности субъекта доступа, а также принадлежности субъекту доступа предъявленного идентификатора и аутентификационной информации.

Примечание – При доступе действия по проверке подлинности, а также принадлежности предъявленного идентификатора и аутентификационной информации осуществляются доверяющей и проверяющей сторонами.

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

7.3 При доступе доказательство подлинности субъекта доступа должно основываться на проверке соответствия аутентификационной информации, предъявленной субъектом доступа, аутентификационной информации, которая ассоциирована с предъявленным идентификатором

доступа у доверяющей стороны. Доказательство принадлежности субъекту идентификатора и аутентификационной информации должно основываться на проверке актуальности (действительности) аутентификационной информации и проверке связи идентификатора и аутентификационной информации с субъектом доступа.

Общая характеристика типового процесса аутентификации приведена в Приложении Б.

7.4 При доступе должна обеспечиваться неизменность субъекта доступа и объекта доступа. В процессе аутентификации (до ее завершения) и субъект доступа, и объект доступа (и третья доверенная сторона, при необходимости) должны иметь возможность удостовериться (убедиться) в их неизменности.

7.5 В процессе аутентификации применяются следующие факторы:

- фактор знания: субъект доступа должен знать определенную информацию;

Примечание – При аутентификации с применением фактора знания может использоваться как аутентификационная информация, непосредственно известная пользователю, например, пароль, графический пароль, изображение, так и информация, позволяющая получить доступ к аутентификационной информации, например, одноразовый пароль или PIN-код;

- фактор владения: субъект доступа должен обладать определенным предметом, содержащим аутентификационную информацию;

Примечание – При аутентификации с применением фактора владения может использоваться, например, устройство аутентификации или механизм, приспособление, вещь, которые содержат аутентификационную информацию;

- фактор биометрический: субъекту доступа должен быть свойственен определенный признак.

Примечания

1 Фактор биометрический применяется при аутентификации субъектов доступа, ассоциированных с физическими лицами.

2 При аутентификации с применением фактора биометрического могут использоваться, например, биометрические данные физического лица или шаблон поведения.

7.6 При доступе к объекту доступа для аутентификации субъекта доступа необходимо использовать один фактор (однофакторная аутентификация) или несколько факторов (многофакторная аутентификация). При многофакторной аутентификации должны совместно применяться не менее двух различных факторов. Доступ к объекту доступа при многофакторной аутентификации должен предоставляться после успешной вторичной идентификации субъекта доступа и положительного результата проверки аутентификационной информации, соответствующей всем совместно используемым факторам аутентификации, без доведения субъекту доступа результатов проверки по каждому фактору аутентификации.

Примечания

1 Примером однофакторной аутентификации пользователя является использование для аутентификации фактора знания с применением в качестве аутентификационной информации пароля, PIN-кода или ответа на вопрос, которые знает пользователь.

2 Примером многофакторной аутентификации пользователя является совместное применение для аутентификации фактора владения (например, пользователь владеет аутентификационной информацией, хранящейся в устройстве аутентификации) и фактора знания (например, пользователь знает пароль, позволяющий использовать аутентификационную информацию, содержащуюся в устройстве аутентификации). Доступ к ресурсам автоматизированной (информационной) системы предоставляется пользователю после его успешной вторичной идентификации и положительного результата проверки аутентификационной информации, соответствующей и фактору владения, и фактору знания.

3 При многошаговой идентификации и аутентификации в рамках отдельных процессов («шагов») идентификации и аутентификации могут использоваться как однофакторная, так и многофакторная аутентификация.

4 Аутентификация условно считается многофакторной при информационном

взаимодействии между субъектом доступа и объектом доступа, которые соответствуют вычислительным процессам (средствам вычислительной техники, автоматизированным (информационным) системам и т.п.), функционирующим в автоматическом режиме. При этом данные вычислительные процессы не ассоциируются с физическим лицом.

7.7 Фактор биометрический должен использоваться только совместно с другими факторами, в том числе для подтверждения фактора владения. При этом применение фактора биометрического в качестве единственного фактора при однофакторной аутентификации не допускается.

Примечание – Порядок и правила применения фактора биометрического при аутентификации определяются соответствующими действующими нормативными правовыми документами и документами по стандартизации.

7.8 В общем случае при аутентификации обмен аутентификационной информацией и другими данными, необходимыми для аутентификации, осуществляется между субъектом доступа, доверенной третьей стороной и объектом доступа с учетом их функциональные ролей. В зависимости от организации обмена аутентификационной информацией и используемых при этом протоколов аутентификации необходимо различать одностороннюю и взаимную аутентификацию.

В односторонней аутентификации участвуют субъект доступа и объект доступа, который считается доверяющей стороной (при необходимости – доверяющей и проверяющей). Односторонняя аутентификация обеспечивает уверенность в подлинности субъекта доступа только у доверяющей стороны. При этом субъект доступа полагает, что доверяющая сторона является подлинной.

В процессе взаимной аутентификации субъект доступа и объект доступа попеременно выполняют функциональную роль доверяющей стороны (при необходимости – доверяющей и проверяющей). При этом взаимная аутентификация обеспечивает уверенность в подлинности другой

стороны и у субъекта доступа, и у объекта доступа.

7.9 Процесс аутентификации может быть организован как с участием доверенной третьей стороны, так и без нее. При односторонней однофакторной аутентификации по паролю услуги доверенной третьей стороны не используются, а регистрирующая, проверяющая и доверяющая стороны объединены в доверяющую сторону и ее функции выполняет объект доступа (см. рисунок 1).

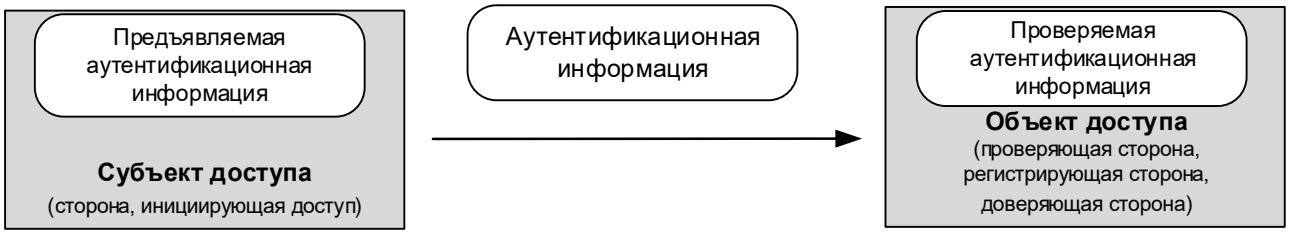

Рисунок 1 – Организация передачи аутентификационной информации при односторонней однофакторной аутентификации по паролю

7.10 При использовании услуг доверенной третьей стороны процесс аутентификации может включать в себя одну доверенную третью сторону или их цепочку. Введение дополнительных единиц доверенных третьих сторон обеспечивает аутентификацию в среде, включающей большое число субъектов доступа, где каждая из доверенных третьих сторон обслуживает только часть субъектов доступа.

При обмене аутентификационной информацией доверенная третья сторона, как проверяющая сторона, может быть посредником между субъектом доступа и объектом доступа (см. рисунок 2).

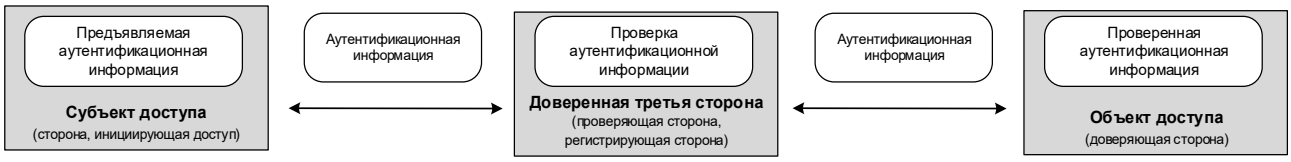

Рисунок 2 – Организация обмена аутентификационной информацией с доверенной третьей стороны в качестве посредника

Доверенная третья сторона, как проверяющая сторона, может не являться прямым участником обмена между субъектом доступа и объектом доступа, но обеспечивать их данными, необходимыми для аутентификации (см. рисунок 3).

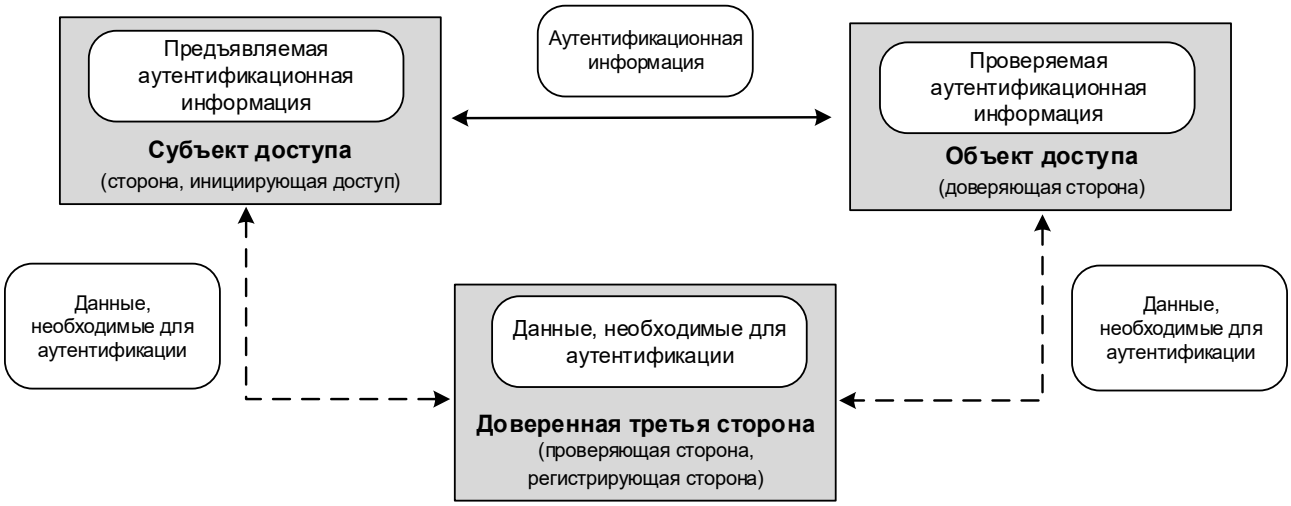

Рисунок 3 – Организация обмена аутентификационной информацией и другими данными, необходимыми для аутентификации, без прямого участия доверенной третьей стороны

При аутентификации в условиях временного отсутствия взаимодействия с доверенной третьей стороной (см. рисунок 4), как проверяющей стороной, объект доступа, как доверяющая сторона, может использовать списки действительных и аннулированных электронных удостоверений или другие методы проверки аутентификационной информации.

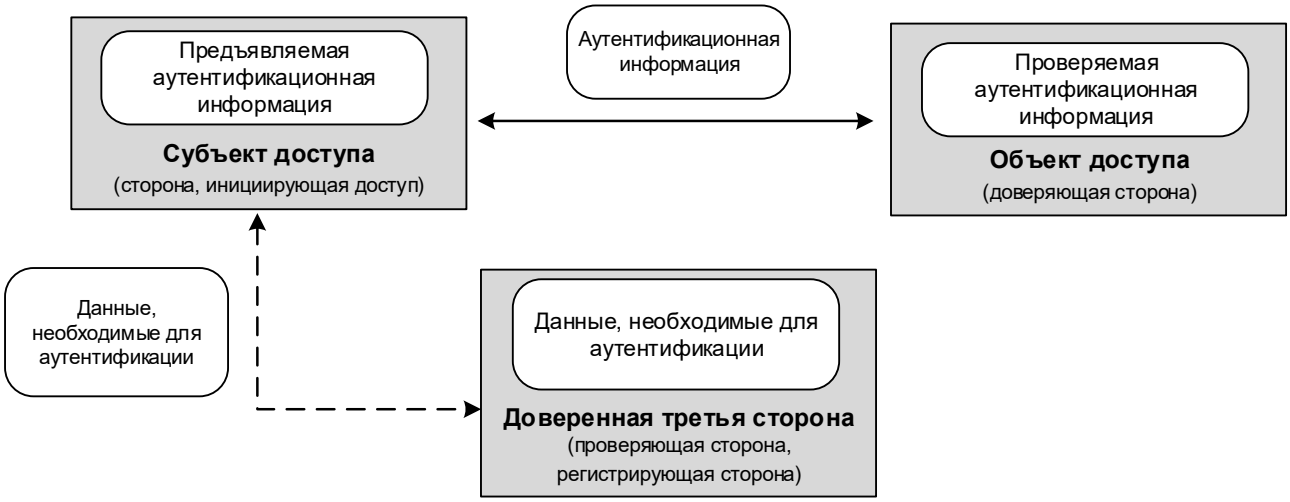

Рисунок 4 – Организация обмена аутентификационной информацией и другими данными, необходимыми для аутентификации, в условиях временного отсутствия взаимодействия объекта доступа с доверенной третьей стороной

7.11 Процесс аутентификации, с учетом действий, выполняемых при идентификации, в общем виде должен включать:

- формирование и регистрацию аутентификационной информации субъекта (объекта) доступа при первичной идентификации. При этом аутентификационная информация может назначаться регистрирующей стороной или самостоятельно формироваться субъектом доступа в соответствии с установленными правилами;

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

- предъявление субъектом доступа доверяющей стороне идентификатора и аутентификационной информации при запросе доступа к объекту доступа;

- проверку подлинности субъекта доступа доверяющей стороной в рамках обмена аутентификационной информацией и другими данными, необходимыми для аутентификации;

- проверку принадлежности субъекту доступа предъявленных идентификатора и аутентификационной информации проверяющей стороной,

включая проверку актуальности (действительности) аутентификационной информации и проверку связи идентификатора и аутентификационной информации с субъектом доступа;

- принятие доверяющей стороной решения о результате аутентификации и последующем проведении авторизации.

7.12 При организации доступа должен использоваться один из видов аутентификации: простая, усиленная или строгая. Каждый из видов аутентификации определяется используемым методом аутентификации.

7.13 При простой аутентификации должна применяться однофакторная односторонняя аутентификация с организацией передачи аутентификационной информации от субъекта доступа к объекту доступа. В процессе простой аутентификации необходимо использовать протоколы аутентификации, соответствующие данной организации передачи аутентификационной информации, в том числе и криптографические.

Примечание – Примером простой аутентификации является использование в качестве аутентификационной информации пароля, который знает пользователь.

7.14 При усиленной аутентификации должны применяться многофакторная односторонняя аутентификация с организацией передачи аутентификационной информации от субъекта доступа к объекту доступа или взаимная аутентификация с организацией обмена аутентификационной информацией между субъектом доступа и объектом доступа. В процессе усиленной аутентификации необходимо использовать протоколы аутентификации, соответствующие данной организации передачи (обмена) аутентификационной информации, в том числе и криптографические.

Примечание

1 Примером усиленной аутентификации является использование при многофакторной односторонней аутентификации пользователя пароля, который знает пользователь, и одноразового пароля, создаваемого с применением устройства аутентификации, находящегося во владении данного пользователя.

2 Примером усиленной аутентификации является использование аутентификационной информации при многофакторной взаимной аутентификации вычислительных процессов, ресурсов и т.п.

7.15 При строгой аутентификации должна применяться многофакторная взаимная аутентификация с организацией двухстороннего, между субъектом доступа и объектом доступа, или многостороннего (при использовании третьей доверенной стороны) обмена аутентификационной информацией. В процессе строгой аутентификации должны использоваться криптографические протоколы аутентификации, соответствующие данной организации обмена, и включающие различные последовательности обмена сообщениями (двух- и многопроходные) между участниками процесса аутентификации.

Примечание – Примером строгой аутентификации является совместное использование при аутентификации закрытого ключа и соответствующего ему электронного удостоверения, содержащего открытый ключ. Электронное удостоверение может формироваться доверенной третьей стороной. Закрытый ключ и соответствующее ему электронное удостоверение, содержащее открытый ключ, хранятся, как правило, с применением устройства аутентификации, находящегося во владении пользователя. При этом пользователь знает пароль или PIN-код, позволяющий использовать данную аутентификационную информацию.

7.16 Аутентификация любого вида, используемая для подтверждения подлинности субъекта доступа, который идентифицирован как анонимный субъект доступа («аноним»), считается анонимной аутентификацией.

Примечание – Как правило, при аутентификации анонимного субъекта доступа используется простая аутентификация.

7.17 При выборе вида аутентификации, применяемого в конкретной среде функционирования, должны учитываться риски информационной безопасности, связанные как со средой обмена аутентификационными сообщениями (или средой функционирования), так и с допустимым харак-

тером действий субъекта доступа, следующих за положительным результатом его аутентификации.

7.18 В зависимости от используемого метода аутентификации для формирования и (или) хранения аутентификационной информации могут применяться соответствующие технические (аппаратные) или виртуальные устройства. При этом используемые устройства аутентификации не должны входить в состав объекта доступа.

Примечание – В качестве устройств аутентификации могут применяться, например, токены, отделённые от автоматизированной (информационной) системы, к которой осуществляется доступ.

Для хранения электронного удостоверения, которое используется для идентификации, и формирования соответствующего закрытого ключа, который используется при аутентификации, рекомендуется применять устройства аутентификации с неизвлекаемым закрытым ключом.

Примеры устройств, применяемых при различных видах аутентификации, приведены в Приложении В.

8 Уровни доверия к результатам идентификации и аутентификации

8.1 Уровень доверия к результатам идентификации определяется достигнутой уверенностью в том, что субъект (объект) доступа действительно соответствует зарегистрированной идентификационной информации, и зависит от результатов вторичной идентификации.

Примечание - Уровень доверия к результатам идентификации для объекта доступа определяется достигнутой уверенностью в результатах первичной идентификации объекта доступа. Уровень доверия к результатам идентификации для субъекта

доступа определяется достигнутой уверенностью в результатах первичной идентификации и зависит от результатов его вторичной идентификации.

Устанавливается три уровня доверия к результатам идентификации:

- низкий уровень доверия. На низком уровне доверия к результатам идентификации существует некоторая уверенность в том, что субъект доступа, зарегистрированный в процессе первичной идентификации и успешно прошедший вторичную идентификацию, действительно соответствует идентификационной информации, которая однозначно определяется предъявленным идентификатором доступа;

- средний уровень доверия. На среднем уровне доверия к результатам идентификации существует умеренная уверенность в том, что субъект доступа, зарегистрированный в процессе первичной идентификации и успешно прошедший вторичную идентификацию, действительно соответствует идентификационной информации, которая однозначно определяется предъявленным идентификатором доступа;

- высокий уровень доверия. На высоком уровне доверия к результатам идентификации существует значительная уверенность в том, что субъект доступа, зарегистрированный в процессе первичной идентификации и успешно прошедший вторичную идентификацию, действительно соответствует идентификационной информации, которая однозначно определяется предъявленным идентификатором доступа.

Если субъект доступа идентифицирован как анонимный субъект доступа («аноним»), то нет никакой уверенности в том, что он действительно соответствует зарегистрированной идентификационной информации, которая определяется предъявленным идентификатором доступа.

Общая характеристика уровней доверия к результатам идентификации приведена в приложении Г (Таблица Г.1).

8.2 Уровень доверия к результатам аутентификации определяется

достигнутой уверенностью в том, что субъект доступа действительно является тем зарегистрированным субъектом доступа, за кого себя выдает предъявленным идентификатором доступа.

Уровень доверия к результатам аутентификации зависит от вида аутентификации при условии соблюдения корректности реализации соответствующих методов и протоколов аутентификации.

Устанавливается три уровня доверия к результатам аутентификации: низкий, средний, высокий.

При использовании простой аутентификации имеется некоторая уверенность в том, что субъект доступа действительно является тем зарегистрированным субъектом доступа, за кого себя выдает предъявленным идентификатором доступа. Данная аутентификация обеспечивает низкий уровень доверия к ее результатам.

При использовании усиленной аутентификации появляется умеренная уверенность в том, что субъект доступа действительно является тем зарегистрированным субъектом доступа, за кого себя выдает предъявленным идентификатором доступа. Данная аутентификация обеспечивает средний уровень доверия к ее результатам.

При использовании строгой аутентификации существует значительная уверенность в том, что и субъект доступа, и объект доступа действительно является тем зарегистрированным субъектом (объектом) доступа, за кого себя выдает предъявленным идентификатором каждый из них. Данная аутентификация обеспечивает высокий уровень доверия.

При аутентификации анонимного субъекта доступа (анонимной аутентификации) уровень доверия к результатам аутентификации определяется используемым видом аутентификации, но при этом нет никакой уверенности в том, что субъект доступа действительно является тем, за кого себя выдает предъявленным идентификатором доступа.

Общая характеристика уровней доверия к результатам аутентификации приведена в приложении Г (Таблица Г.2).

8.3 Уровень доверия к результатам идентификации и аутентификации определяется уровнем доверия к результатам идентификации и уровнем доверия к результатам аутентификации (Таблица 1).

Таблица 1 – Определение уровня доверия к результатам идентификации и аутентификации

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

Уровень доверия к результатам идентификации и аутентификации, который должен быть достигнут в конкретной среде функционирования, должен устанавливаться в соответствии с действующими нормативными правовыми документами на основе результатов анализа рисков информационной безопасности, выполняемого в соответствии с ГОСТ Р ИСО/МЭК 27005-2010.

Приложение А

(справочное)

Взаимосвязь терминов, входящих в группы, относящиеся к понятиям «идентификация» и «аутентификация»

Взаимосвязь терминов, входящих в группы, относящиеся к понятиям «идентификация» и «аутентификация» представлена на рисунках А.1 и А.2. Обозначения связей между терминами соответствует установленным соглашениям [8].

Настоящий стандарт не является терминологическим [9], поэтому группы, относящиеся к понятиям «идентификация» и «аутентификация», не выделены в отдельные подразделы в составе раздела 3.

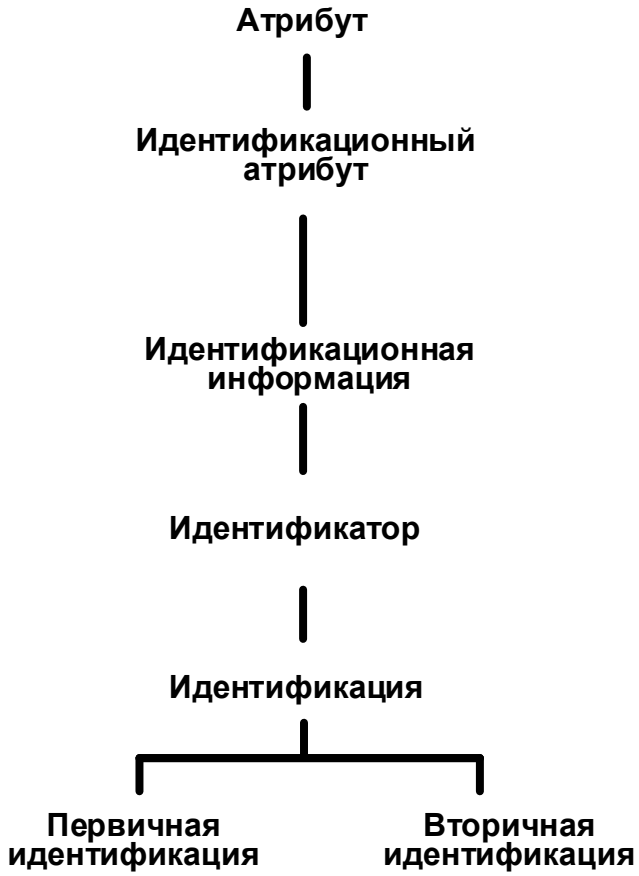

Рисунок А.1 – Схема взаимосвязи терминов, входящих в группу, относящуюся к понятию «идентификация»

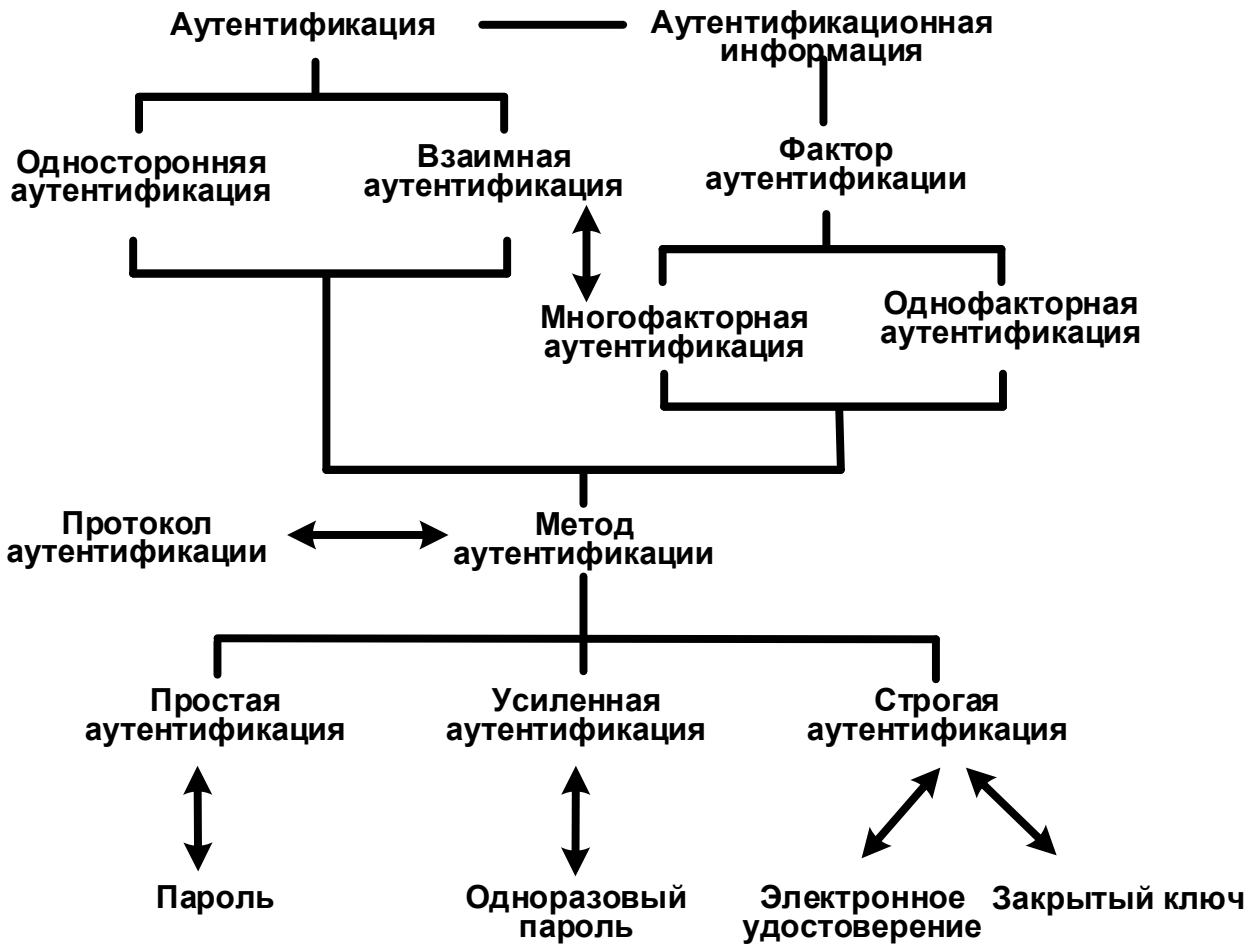

Рисунок А.2 - Схема взаимосвязи терминов, входящих в группу, относящуюся к понятию «аутентификация»

Приложение Б

(справочное)

Общая характеристика типовых процессов идентификации и аутентификации

Для того, чтобы сторона В при информационном взаимодействии предоставила доступ стороне А, запросившей доступ, сначала проводится процесс вторичной идентификации. Сторона А предъявляет стороне В идентификатор доступа, а сторона В выполняет проверку с использованием верификатора (см. рисунок Б.1).

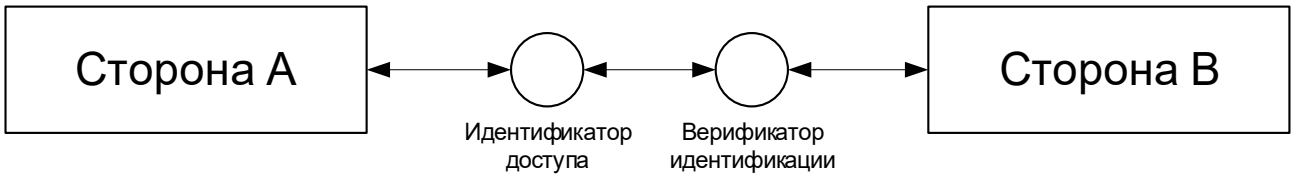

Рисунок Б.1 – Общая схема проверки идентификационной информации

Назначение верификатора идентификации состоит в реализации двух функций:

– опознавание стороны А путем проверки существования (наличия) предъявленного идентификатора в перечне зарегистрированных при первичной идентификации;

– проверка принадлежности идентификатора стороне А, в том числе его актуальности (действительности).

В случае положительного результата проверки за процессом идентификации осуществляется аутентификация стороны А. В процессе аутентификации сторона А предъявляет стороне В аутентификационную информацию. Для ее проверки сторона В должна иметь доверенный для обеих сторон верификатор аутентификации (см. рисунок Б.2).

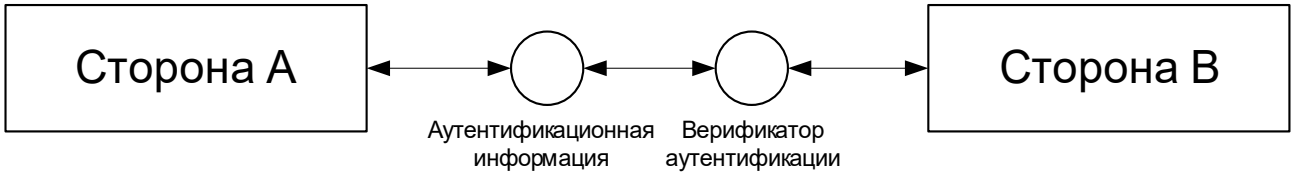

Рисунок Б.2 – Общая схема проверки аутентификационной информации

Назначение верификатора аутентификации состоит в реализации двух функций:

- проверка подлинности стороны А с помощью аутентификационной информации;

- проверка принадлежности аутентификационной информации стороне А, в том числе ее актуальности (действительности).

В случае положительного результата проверки процесс аутентификации считается успешно пройденным.

Упрощенная схема типового процесса первичной идентификации субъекта доступа представлена на рисунке Б.3.

Упрощенная схема типовых процессов вторичной идентификации и аутентификации субъекта доступа, который является пользователем, представлена на рисунке Б.4, а схема процессов вторичной идентификации и аутентификации субъекта доступа, который является ресурсом, представлена на рисунке Б.5.

Приведенные схемы могут рассматриваться как базис для построения процессов идентификации и аутентификации. Непосредственная их реализация в средствах защиты от несанкционированного доступа, средствах вычислительной техники и автоматизированных (информационных) системах должна осуществляться в соответствии с требованиями нормативных документов и учитывать положения ГОСТ Р 56939–2016.

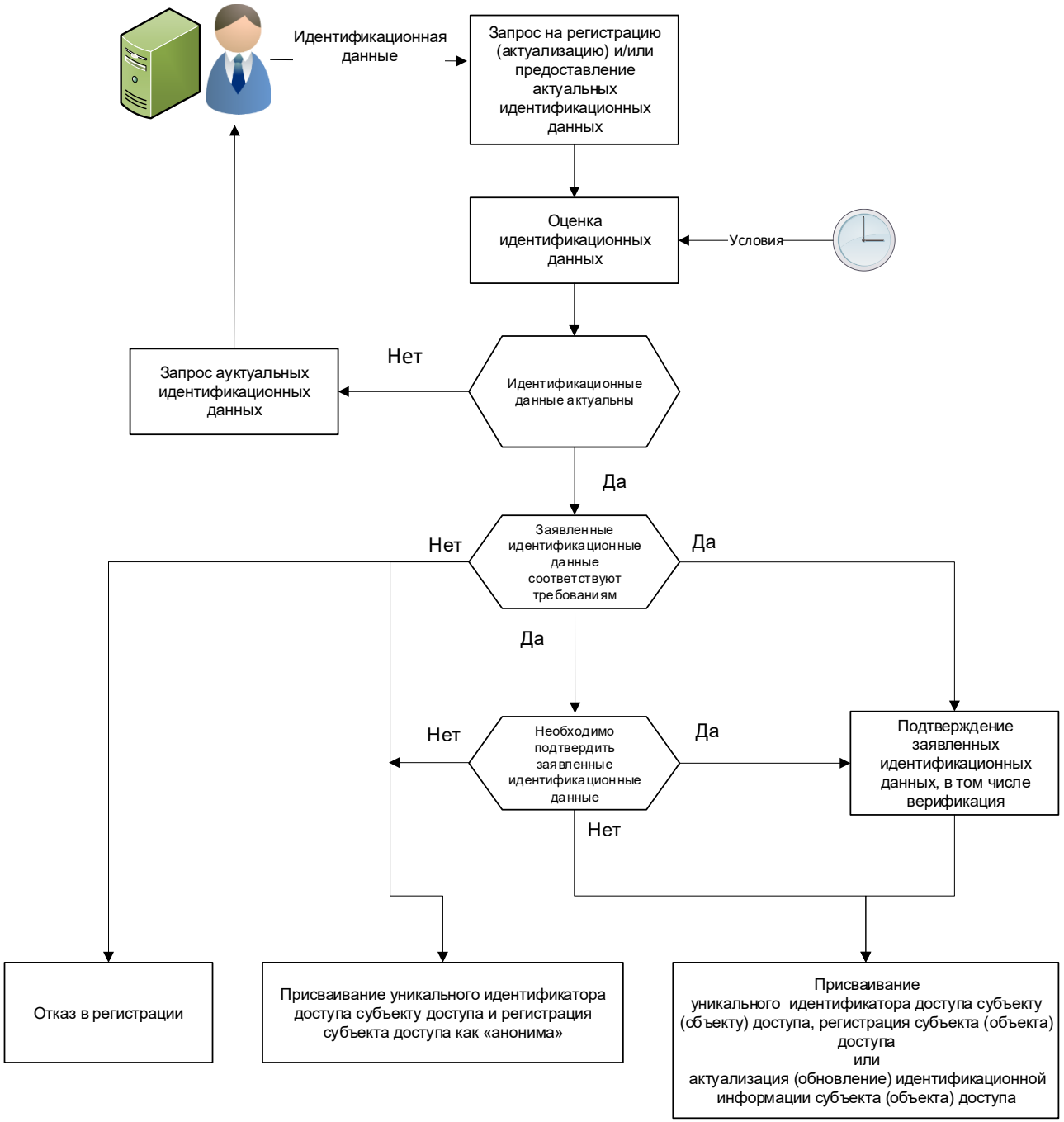

Рисунок Б.3 – Упрощенная схема типового процесса первичной идентификации

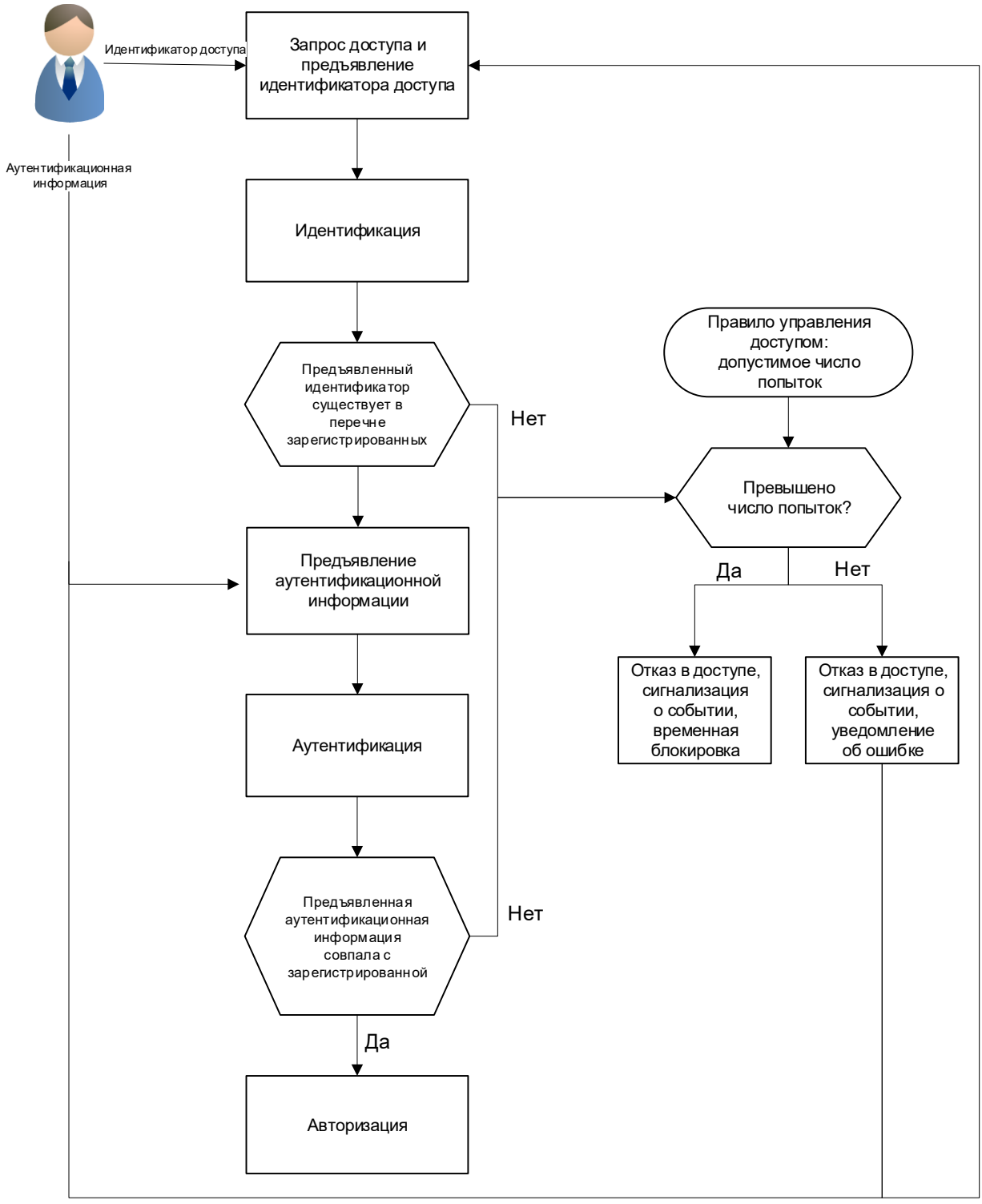

Рисунок Б.4 – Упрощенная схема типовых процессов вторичной идентификации и аутентификации субъекта доступа, который является пользователем

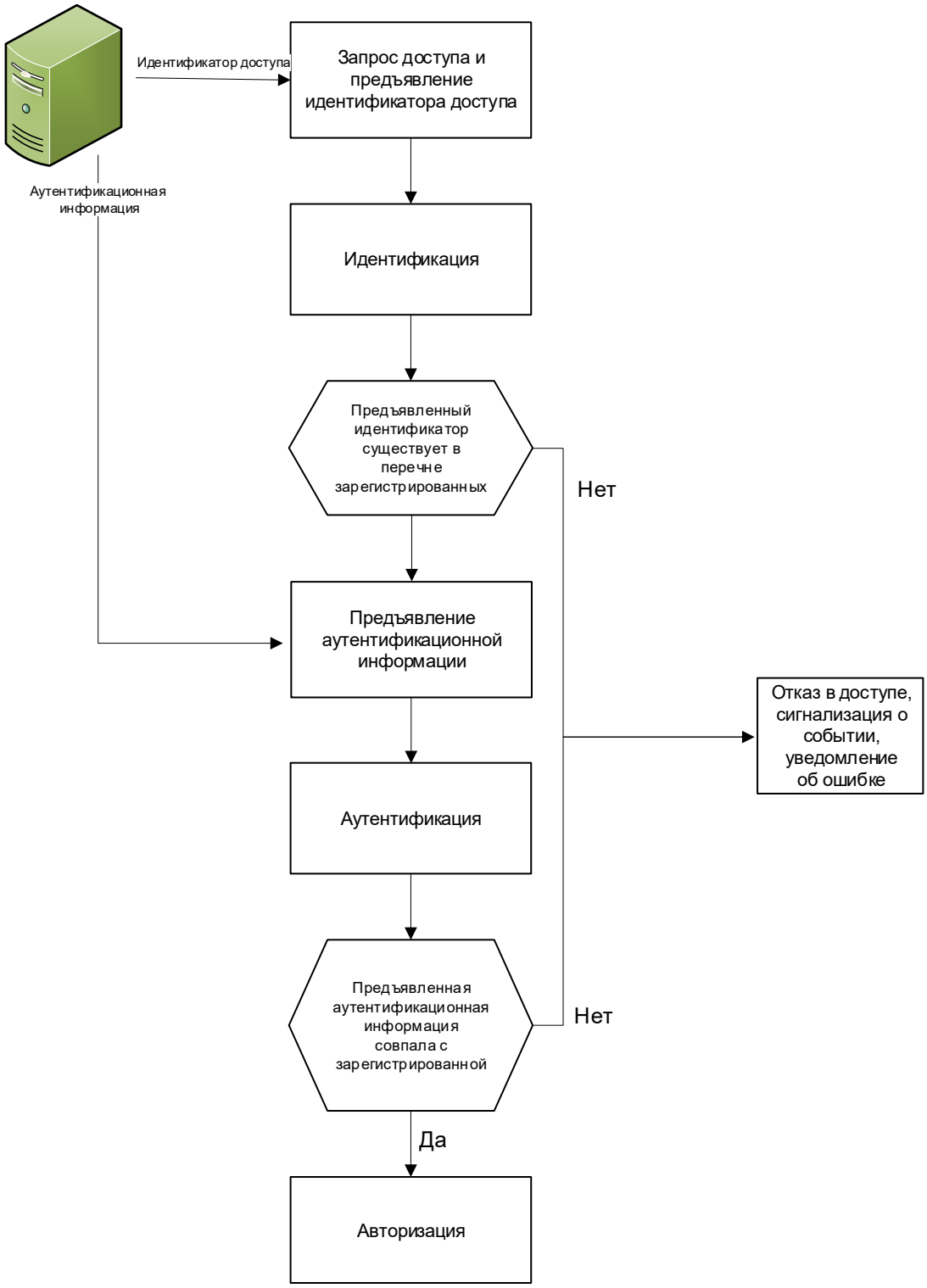

Рисунок Б.5 – Упрощенная схема типовых процессов вторичной идентификации и аутентификации субъекта доступа, который является ресурсом

Приложение В

(справочное)

Примеры устройств, применяемых при различных видах аутентификации

В.1 Устройства аутентификации, применяемые при простой аутентификации:

- изделия класса «Touch memory» или аналоги;

- карты с магнитной полосой;

- генератор одноразовых паролей;

- флэш-накопители.

В.2 Устройства аутентификации, применяемые при усиленной аутентификации:

- скрэтч-карты с предустановленным случайным числом;

- генератор одноразовых паролей;

- токены форм-фактора «Смарт-карта» или «USB-ключ».

В.3 Устройства аутентификации, применяемые при строгой аутентификации:

- токены форм-фактора «Смарт-карта» или «USB-ключ» с возможностью хранения закрытого ключа внутри устройства. Память устройства защищена паролем или PIN-кодом;

- токены форм-фактора «Смарт-карта» или «USB-ключ» с возможностью генерации ключевой пары внутри устройства. Память устройства защищена паролем или PIN-кодом.

Примечания

1 В состав устройств аутентификации, могут быть включены компоненты, использующие фактор биометрический для подтверждения фактора владения устройством.

2 В перечне устройства аутентификации приведены по защищённости от клонирования устройства (и содержащейся в нем аутентификационной информации), а также возможности компрометации закрытого ключа, используемого для аутентификации.

3 Перечень примеров не является исчерпывающим и, в связи с развитием технологий, может изменяться. Другие, не включенные в перечень устройства, могут

иметь как большую, так и меньшую защищенность от клонирования устройства (и содержащейся в нем аутентификационной информации), а также возможности по предотвращению компрометации закрытого ключа, используемого при аутентификации.

Приложение Г

(справочное)

Общая характеристика уровней доверия к результатам идентификации и аутентификации

Таблица Г.1 – Общая характеристика уровней доверия к результатам идентификации

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

Таблица Г.2 – Общая характеристика уровней доверия к результатам аутентификации

Метод аутентификации субъекта (объекта) доступа			Вид аутентификации субъекта (объекта) доступа	Уверенностью в том, что субъект и (или) объект доступа действительно является тем субъектом (объектом) доступа, за кого себя выдает	Уровень доверия к результатам аутентификации субъекта (объекта) доступа
Однофакторная аутентификация	Односторонняя аутентификация	Соответствующие протоколы аутентификации, в том числе и криптографические	Простая	Некоторая уверенность	Низкий уровень доверия
Многофакторная аутентификация	Односторонняя или взаимная аутентификация	Соответствующие протоколы аутентификации, в том числе и криптографические	Усиленная	Умеренная уверенность	Средний уровень доверия
Многофакторная аутентификации	Взаимная аутентификация	Криптографические протоколы аутентификации	Строгая	Значительная уверенность	Высокий уровень доверия
Примечание – При аутентификации анонимного субъекта доступа (анонимной аутентификации), как правило используется простая аутентификация, чем достигается низкий уровень доверия к ее результатам, но при этом нет никакой уверенности в том, что субъект доступа действительно является тем, за кого себя выдает.					

Библиография

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

[2] ITU-T Rec.X.810 (11/1995) Series X — Информационная технология. Взаимосвязь открытых систем. Основы безопасности для открытых систем: обзор (Information technology – Open Systems Interconnection – Security frameworks for open systems: Overview)

[3] Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»

[4] ИСО/МЭК 18033-1:2015 (ISO/IEC 18033-1:2015) — Информационная технология. Методы и средства обеспечения безопасности. Алгоритмы кодирования. Часть 1. Общие положения (Information technology -- Security techniques -- Encryption algorithms -- Part 1: General)

[5] Федеральный закон от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи»

[6] ГОСТ Р 34.12-2015 — Информационная технология. Криптографическая защита информации. Блочные шифры

[7] European Standard 319 411:2016 — Электронные подписи и инфраструктуры. Политика и требования безопасности к доверенным сервис-провайдерам, выпускающим сертификаты. Часть

		1 Основные требования (Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements)
[8]	ГОСТ Р ИСО 704–2010	Терминологическая работа. Принципы и методы
[9]	ГОСТ Р ИСО 10241-1–2013	Терминологические статьи в стандартах. Часть 1. Общие требования и примеры представления

УДК 004 ОКС 35.030

Ключевые слова: защита информации, идентификация и аутентификация, управление доступом, первичная идентификация, вторичная идентификация, аутентификация, доверие к результатам идентификации, доверие к результатам аутентификации