ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 70262.1— 2022

Защита информации

ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ

Уровни доверия идентификации

Издание официальное

Москва
Российский институт стандартизации
2022

gost.e-ecolog.ru

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 ТК 362 «Защита информации»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 5 августа 2022 г. № 740-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 «РСТ», 2022

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 7
5 Первичная идентификация 8
5.1 Общие требования к первичной идентификации 8
5.2 Подтверждение идентификационных данных при первичной идентификации 10
5.3 Уровни доверия первичной идентификации 12
5.4 Общий порядок первичной идентификации 12
6 Вторичная идентификация 14
7 Уровни доверия идентификации 14
Приложение А (справочное) Общая характеристика уровней доверия первичной идентификации . . . 16
Библиография 17

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.

В автоматизированной (информационной) системе физическое лицо, являющееся пользователем, при использовании информационных и вычислительных ресурсов выполняет операции по обработке данных через вычислительные процессы, что порождает риски неоднозначного сопоставления конкретного вычислительного процесса конкретному физическому лицу и конкретному ресурсу. 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 соответствия как между физическим лицом и вычислительными процессами, которыми оно представлено при выполнении операций, так и между вычислительными процессами и ресурсами средств вычислительной техники. Данное соответствие, как правило, устанавливается при регистрации ресурса как объекта или субъекта доступа и физического лица как пользователя (субъекта доступа), проверяется при опознавании пользователя по предъявленному идентификатору доступа и обеспечивает определенную уверенность в том, что обработка данных вычислительными процессами действительно осуществляется от имени физического лица (или ресурса), имеющего на это соответствующие права[1)].

При подготовке настоящего стандарта учитывались нормы, определенные ГОСТ Р 58833, а также правила идентификации, установленные ГОСТ ISO/IEC 24760-2, ГОСТ Р 59515 с учетом [1], [2].

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

[1)] Уверенность в том, что обработка данных вычислительными процессами действительно осуществляется от имени физического лица (или ресурса), имеющего на это соответствующие права, обеспечивается при условии положительного результата проверки его подлинности (аутентификации).

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Защита информации

ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ

Уровни доверия идентификации

Information protection.
Identification and authentication.
Identification results assurance levels

Дата введения — 2023—01—01

1 Область применения

Настоящий стандарт устанавливает единообразную организацию процесса идентификации субъектов и объектов доступа в средствах защиты информации, средствах вычислительной техники и автоматизированных (информационных) системах, а также определяет общие правила идентификации, обеспечивающие необходимую уверенность в ее результатах.

Настоящий стандарт определяет состав участников и основное содержание процесса идентификации, рекомендуемые 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.

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

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 ISO/IEC 24760-2 Информационные технологии. Методы и средства обеспечения безопасности. Основы управления идентичностью. Часть 2. Базовая архитектура и требования

ГОСТ Р 50922 Защита информации. Основные термины и определения

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

ГОСТ Р 59515 Информационные технологии. Методы и средства обеспечения безопасности. Подтверждение идентичности

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 указателю «Национальные стандарты», который опубликован по состоянию на 1 января текущего года, и по выпускам

Издание официальное

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, а также следующие термины с соответствующими определениями:

3.1

анонимный субъект доступа; аноним: Субъект доступа, первичная идентификация которого выполнена в конкретной среде функционирования, но при этом его идентификационные данные не соответствуют требованиям к первичной идентификации или не подтверждались.

[ГОСТ Р 58833—2020, пункт 3.1]

3.2

атрибут (субъекта [объекта] доступа): Признак или свойство субъекта доступа или объекта доступа.

[ГОСТ Р 58833—2020, пункт 3.2]

3.3

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.

[ГОСТ Р 58833—2020, пункт 3.4]

3.4

верификация: Процесс проверки информации путем сопоставления предоставленной информации с ранее подтвержденной информацией.

[ГОСТ Р 58833—2020, пункт 3.9]

3.5 **верифицирующая сторона:** Сторона, которая осуществляет верификацию идентификационных данных.

3.6 **вспомогательный атрибут (субъекта [объекта] доступа):** Атрибут, который не является идентификационным атрибутом, но может использоваться при подтверждении идентификационных данных субъекта доступа или объекта доступа.

Примечание — Вспомогательный атрибут, как правило, используется для подтверждения существования идентификационного атрибута субъекта доступа или объекта доступа.

3.7

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]

3.8

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]

3.9

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 — Доверие рассматривается в качестве основания для уверенности.

3.10

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]

3.11

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]

3.12

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

[ГОСТ Р 58833—2020, пункт 3.21]

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

3.13

идентификационные данные: Совокупность идентификационных атрибутов и их значений, которая связана с конкретным субъектом доступа или конкретным объектом доступа.

Примечание — При первичной идентификации идентификационные данные, как правило, предоставляются субъектом доступа, ассоциированным с физическим лицом, или получаются возможным (доступным) способом от субъекта доступа, ассоциированного с ресурсом, и объекта доступа. Указанные идентификационные данные считаются идентификационными данными, заявленными субъектом (объектом) доступа (заявленными идентификационными данными).

[ГОСТ Р 58833—2020, пункт 3.22]

Примечания

1 Идентификационные данные, которые подтверждены в соответствии с устанавливаемыми требованиями к первичной идентификации, считаются подтвержденными идентификационными данными.

2 Идентификационные данные включают идентификационные атрибуты, которые могут быть неотчуждаемыми или отчуждаемыми от субъекта (объекта) доступа, и их значения, которые, как правило, являются отчуждаемыми.

3.14

идентификационный атрибут: Атрибут, который характеризует субъект доступа или объект доступа и может быть использован для его распознавания.

[ГОСТ Р 58833—2020, пункт 3.23]

3.15

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

[[3], 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

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

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

3.18

неотказуемость (non-repudiation): Способность удостоверять имевшее место действие или событие так, чтобы эти события или действия не могли быть позже отвергнуты.

[ГОСТ Р ИСО/МЭК 13335-1—2006, пункт 2.16]

3.19

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.

[[4], статья 2]

3.20

объект доступа: Одна из сторон информационного взаимодействия, предоставляющая доступ.

[ГОСТ Р 58833—2020, пункт 3.33]

3.21

объективное свидетельство (objective evidence): Данные, подтверждающие наличие или истинность чего-либо.

Примечания

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

2 Объективное свидетельство для цели аудита обычно включает записи, изложение фактов или другую информацию, которые имеют отношение к критериям аудита и могут быть проверены.

[ГОСТ Р ИСО 9000—2015, пункт 3.8.3]

3.22

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.

[Адаптировано из [4], статья 2]

3.23 **официальное свидетельство:** Свидетельство идентичности, содержащее идентификационные атрибуты и/или значения идентификационных атрибутов, управление которыми осуществляет полномочная сторона.

Примечание — Официальное свидетельство для конкретного идентификационного атрибута может быть подтверждающим свидетельством для другого идентификационного атрибута.

3.24

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]

3.25

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

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

3.26

подтверждающая информация: Информация, собранная и использованная для подтверждения идентификационных данных в соответствии с установленными требованиями к первичной идентификации.

[ГОСТ Р 58833—2020, пункт 3.43]

Примечание — Подтверждающая информация используется как доказательство для уверенности в результатах первичной идентификации.

3.27 **подтверждающее свидетельство:** Свидетельство идентичности, содержащее идентификационные атрибуты (значения идентификационных атрибутов), управление которыми не осуществляет полномочная сторона.

Примечание — Подтверждающее свидетельство, как правило (но не обязательно), содержит вспомогательные атрибуты.

3.28

политика информационной безопасности (организации): Формальное изложение правил поведения, процедур, практических приемов или руководящих принципов в области информационной безопасности, которыми организация руководствуется в своей деятельности.

[Адаптировано из ГОСТ Р 53114—2008, статья 3.2.18]

3.29 **полномочная [верифицирующая] сторона:** Сторона, которая обладает общепризнанным правом управления идентификационными атрибутами и их значениями.

Примечания

1 Управление идентификационными атрибутами (значениями идентификационных атрибутов) может включать, например, создание, изменение, удаление, выпуск, отзыв, верификацию, подтверждение и другие аналогичные действия над ними.

2 В качестве полномочной стороны для субъектов доступа, которые ассоциированы с физическими лицами, может рассматриваться организация, в соответствии с нормативными правовыми актами имеющая право управления идентификационными данными. К таким организациям относятся, например, федеральные, региональные и муниципальные органы исполнительной власти.

3 В качестве полномочной стороны для субъектов доступа, которые не ассоциированы с физическими лицами, могут рассматриваться: организация (например, производитель устройства), администратор автоматизированной (информационной) системы, устройство [средство вычислительной техники, автоматизированная (информационная) система], которые в области действия единых правил управления доступом обладают признанным правом управления идентификационными данными.

3.30

правила управления доступом: Правила, регламентирующие условия доступа субъектов доступа к объектам доступа на основе прав доступа.

Примечания

1 Права доступа определяют набор возможных действий, которые субъекты доступа могут выполнять над объектами доступа в конкретной среде функционирования.

2 Условия доступа определяют перечень действующих прав доступа субъектов доступа к объектам доступа (перечень существующих разрешенных (запрещенных) действий субъектов доступа над объектами доступа) в конкретной среде функционирования.

3 Правила управления доступом могут устанавливаться нормативными правовыми актами, обладателем информации или оператором.

[ГОСТ Р 58833—2020, пункт 3.45]

3.31 **привязка (идентификационных данных):** Установление и/или проверка связи идентификационных данных с заявившим (предоставившим) их субъектом (объектом) доступа.

Примечание — При привязке может использоваться подтверждающая информация, идентификационная информация, идентификационные атрибуты, идентификационные данные, которые известны (свойственны) субъекту доступа, ассоциированному с физическим лицом, а также которые свойственны субъекту доступа, ассоциированному с ресурсом, и объекту доступа.

3.32

процедура (procedure): Установленный способ осуществления деятельности или процесса.

Примечание — Процедуры могут быть документированными или нет.

[ГОСТ Р ИСО 9000—2015, пункт 3.4.5]

3.33

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

[ГОСТ Р ИСО 9000—2015, пункт 3.4.1]

3.34

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

[[5], пункт А.20]

3.35

санкционирование доступа; авторизация: Предоставление субъекту доступа прав на доступ, а также предоставление доступа в соответствии с установленными правилами управления доступом.

[ГОСТ Р 58833—2020, пункт 3.50]

3.36 **свидетельство (идентичности):** Объективное свидетельство, обеспечивающее уверенность в том, что идентификационные данные действительно соответствуют (принадлежат) субъекту доступа или объекту доступа.

Примечание — В качестве свидетельств идентичности могут рассматриваться, например, результаты верификации заявленных идентификационных данных, документальные подтверждения (официальные документы), в том числе и полученные от субъекта (объекта) доступа, а также другая подтверждающая информация.

3.37

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 граничное условие среды функционирования.

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

[ГОСТ Р 58833—2020, пункт 3.53]

3.38

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]

3.39

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]

3.40

управление доступом: Предоставление санкционированного и предотвращение несанкционированного доступа.

[ГОСТ Р 58833—2020, пункт 3.57]

3.41

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]

4 Общие положения

4.1 Процесс идентификации должен включать действия по подготовке, формированию и регистрации идентификационной информации субъекта (объекта) доступа, а также присвоению и регистрации идентификатора субъекта (объекта) доступа в перечне(ях) идентификаторов доступа, а при доступе субъекта доступа к объекту доступа — действия по проверке существования (наличия) идентификатора, предъявленного субъектом доступа, в перечне присвоенных идентификаторов доступа.

4.2 В общем случае с учетом особенностей, определенных ГОСТ Р 58833, идентификация должна включать:

- первичную идентификацию субъекта (объекта) доступа, которая охватывает установление (подтверждение) соответствия между субъектом (объектом) доступа и заявленными им идентификационными данными, формирование идентификационной информации на основе подтвержденных идентификационных данных, присвоение идентификатора доступа субъекту (объекту) доступа и их регистрацию;
- хранение и поддержание актуального состояния (обновление) идентификационной информации субъекта (объекта) доступа в соответствии с установленными правилами;

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

В общем случае первичная идентификация должна осуществляться однократно. 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.

Вторичную идентификацию необходимо повторять при каждом запросе субъекта доступа на доступ к объекту доступа. В течение информационного взаимодействия между субъектом доступа и объектом доступа вторичная идентификация субъекта доступа может выполняться однократно или, при необходимости, с установленной периодичностью.

4.3 Состав участников процесса идентификации и их функциональные возможности (роли) определяются ГОСТ Р 58833. При идентификации, в общем случае, взаимодействуют субъект доступа, регистрирующая и доверяющая стороны. При этом регистрирующая сторона осуществляет первичную идентификацию и хранение идентификационной информации, а доверяющая сторона — вторичную идентификацию субъекта доступа. Дополнительно в первичной идентификации могут участвовать объект доступа и/или стороны, которые имеют следующие функциональные возможности (роли):

- верифицирующая сторона. Основной задачей данной стороны является верификация по запросам регистрирующей стороны заявленных идентификационных данных субъекта (объекта) доступа и их подтверждение свидетельствами;

- полномочная верифицирующая сторона (полномочная сторона). Основной задачей полномочной стороны является управление идентификационными данными, в том числе верификация заявленных идентификационных данных субъекта (объекта) доступа по запросам регистрирующей стороны и их подтверждение официальными свидетельствами.

4.4 Участники процесса идентификации должны обеспечивать защиту информации, используемой при идентификации. При этом состав и содержание мер защиты информации в конкретной среде функционирования следует определять в соответствии с нормативными правовыми актами и документами по стандартизации.

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

4.6 Для конкретной среды функционирования уверенность в том, что субъект доступа, осуществляющий доступ к объекту доступа, действительно соответствует зарегистрированной идентификационной информации, определяется уровнем доверия первичной идентификации субъекта (объекта) доступа и зависит от результатов вторичной идентификации субъекта доступа.

5 Первичная идентификация

5.1 Общие требования к первичной идентификации

5.1.1 Целью первичной идентификации является распознавание субъекта (объекта) доступа посредством установления (подтверждения) соответствия между субъектом (объектом) доступа и заявленными им идентификационными данными.

5.1.2 В результате первичной идентификации субъекту (объекту) доступа присваивается уникальный идентификатор доступа, который однозначно определяет соотнесенную с ним зарегистрированную идентификационную информацию. При этом уникальность идентификатора доступа должна обеспечиваться в области действия единых правил управления доступом. При необходимости в конкретной среде функционирования субъект (объект) доступа может иметь несколько идентификаторов доступа, каждый из которых должен быть уникальным для конкретных условий их использования.

5.1.3 Первичная идентификация должна осуществляться на основании минимально необходимого объема идентификационных атрибутов субъекта (объекта) доступа в соответствии с требованиями к первичной идентификации, устанавливаемыми для области действия единых правил управления доступом.

Примечания

1 В качестве идентификационных атрибутов субъекта доступа, ассоциированного с физическим лицом, могут использоваться, например, фамилия, имя, отчество; дата рождения; адрес места рождения (место рождения); фамилии, имена, отчества родителей; биометрические характеристики; адрес проживания (нахождения); номера телефонов; идентификационные номера, присвоенные организациями, которые являются полномочными сторонами, и т. п. В качестве вспомогательных атрибутов физического лица могут использоваться, например, данные об участии в общественных организациях, номера, являющиеся ссылками на подтверждающие свидетельства, данные из автоматизированных систем, в которых субъект доступа имеет регистрацию, и т. п.

2 В качестве идентификационных атрибутов объекта доступа и субъекта доступа, не ассоциированного с физическим лицом, могут рассматриваться, например, номер сессии, имя пути, унифицированное имя вычислительного ресурса, унифицированный указатель информационного ресурса и т. п., а также использоваться уникальные идентификационные номера, присвоенные производителями устройств.

3 Правила управления доступом (единые правила управления доступом) могут быть реализованы в рамках конкретной среды функционирования, например, в границах: одного или нескольких вычислительных процессов; одного или нескольких средств вычислительной техники; одной или нескольких автоматизированных (информационных) систем. В общем случае единые правила управления доступом и определяют границы конкретной среды функционирования.

5.1.4 Требования к первичной идентификации субъектов (объектов) доступа должны устанавливаться обладателем информации или оператором на основе положений нормативных правовых актов, нормативных документов и документов по стандартизации с учетом особенностей конкретной среды функционирования. При этом состав и содержание устанавливаемых требований должны обеспечить первичную идентификацию субъекта (объекта) доступа с уверенностью, необходимой в данной среде функционирования.

Примечание — Требования к первичной идентификации субъектов (объектов) доступа допускается оформлять в виде отдельных документированных процедур (политик) и/или включать в политику информационной безопасности организации.

5.1.5 Требования к первичной идентификации должны содержать:

- уровень доверия, который должен быть реализован при первичной идентификации;
- характеристику среды функционирования, для которой осуществляется первичная идентификация субъекта доступа, результаты которой признаются правильными (достоверными);
- объем, состав и обязательность идентификационных атрибутов субъекта (объекта) доступа. Объем идентификационных атрибутов, при котором обеспечивается выполнение требований к первичной идентификации и однозначная идентификация субъекта (объекта) доступа, должен быть минимально необходимым [6];
- объем, состав и необходимость использования вспомогательных атрибутов субъекта (объекта) доступа;
- состав значений идентификационных атрибутов, для которых должна быть обеспечена уникальность, порядок действий при ее нарушении, а также возможность использования значений вспомогательных атрибутов для обеспечения уникальности идентификационной информации;
- состав, содержание и порядок сбора подтверждающей информации, а также действия регистрирующей стороны при ее недостаточности;
- порядок и правила верификации заявленных идентификационных данных или идентификационной информации, которая получена из свидетельств, имеющихся у субъекта (объекта) доступа;
- состав необходимых свидетельств идентичности, порядок и правила их представления, рассмотрения, проверки и использования регистрирующей стороной, а также порядок действий при выявлении несоответствий;
- порядок и правила привязки заявленных идентификационных данных к субъекту (объекту) доступа, а также особенности привязки субъектов доступа и объектов доступа в конкретной среде функционирования;
- правила хранения и поддержания актуального состояния (обновление) идентификационной информации субъекта (объекта) доступа;
- возможность и порядок регистрации субъектов доступа, идентификационные данные которых не соответствуют установленным требованиям.

5.1.6 При первичной идентификации субъект (объект) доступа для различных сред функционирования может заявлять различные идентификационные данные, которые должны отвечать требованиям к первичной идентификации, установленным для соответствующей среды функционирования.

5.1.7 При первичной идентификации следует выполнять проверку уникальности значений отдельных идентификационных атрибутов или всей идентификационной информации. Проверка на уникальность обеспечивает уверенность в том, что каждый субъект (объект) доступа будет идентифицирован и внесен в перечень субъектов (объектов) доступа только один раз, то есть в конкретной среде функционирования каждый субъект (объект) доступа будет иметь единственный набор значений идентификационных атрибутов, связанный с идентификатором доступа.

Примечание — Для обеспечения уникальности идентификационной информации физических лиц могут использоваться идентификационные атрибуты, значения которых общеизвестно считаются единственными для физического лица, например, номер документа, удостоверяющего личность его владельца, или страховой номер индивидуального лицевого счета физического лица.

5.1.8 Состав идентификационных атрибутов, для которых в конкретной среде функционирования должна обеспечиваться уникальность значений, устанавливается требованиями к первичной идентификации.

5.2 Подтверждение идентификационных данных при первичной идентификации

5.2.1 Для формирования идентификационной информации субъекта (объекта) доступа в конкретной среде функционирования следует использовать подтвержденные идентификационные данные. В процессе подтверждения необходимо проверить существование заявленных идентификационных данных путем верификации и выполнить их привязку (установить или проверить связь) к субъекту (объекту) доступа.

5.2.2 Верификация заявленных идентификационных данных обеспечивает уверенность в том, что идентификационные данные действительно соответствуют (принадлежат) субъекту (объекту) доступа, который их заявил, при этом идентификационные атрибуты субъекта (объекта) доступа фактически существуют и их значения являются достоверными. Результатом верификации заявленных идентификационных данных являются свидетельства идентичности.

Примечание — Верификация может осуществляться как по запросам регистрирующей стороны непосредственно при подтверждении заявленных идентификационных данных, так и выполняться заблаговременно (вне условий, связанных с подтверждением), и ее результаты в виде свидетельств могут представляться субъектом (объектом) доступа при подтверждении.

Свидетельства идентичности могут представлять собой:

- подтверждающую информацию, предоставленную субъектом (объектом) доступа или другими источниками;
- документальное подтверждение, содержащее верифицированные идентификационные данные субъекта (объекта) доступа или подтверждающую информацию, связанную с ним;
- источники данных, содержащие подтверждающую информацию субъекта (объекта) доступа.

Примечания

1 В качестве свидетельства, представляющего собой подтверждающую информацию, может рассматриваться, например, номер телефона подвижной радиотелефонной связи физического лица или значение уникального идентификационного номера устройства, присвоенного его производителем.

2 В качестве свидетельства, представляющего собой документальное подтверждение, может рассматриваться, например, документ установленного образца, выданный полномочной стороной физическому лицу в порядке, определенном нормативными правовыми актами, или документ установленной формы, поставляемый производителем вместе с устройством.

3 В качестве свидетельства, представляющего собой источник данных, может рассматриваться, например, реестр органа исполнительной власти, в котором зафиксированы значения идентификационных атрибутов физического лица, устройства или программного средства.

5.2.3 При использовании свидетельств необходимо принимать во внимание, что не все свидетельства идентичности могут быть использованы для подтверждения идентификационных данных вне условий, для которых они предназначались. Кроме того, надо учитывать, что отдельные свидетельства могут основываться на результатах предыдущего подтверждения идентификационных данных. При рассмотрении данных свидетельств должна быть оценена возможность их принятия для текущего подтверждения в используемой среде функционирования, а при необходимости — и для последующих аналогичных подтверждений.

5.2.4 При рассмотрении свидетельств и определении возможности их применения в конкретной среде функционирования необходимо, как минимум, учитывать:

- исходную подтвержденность и действительность идентификационных данных: при подтверждении следует использовать свидетельства, базирующиеся на реальных исходных фактах и событиях (или биометрических данных физических лиц), а идентификационные данные на момент применения должны являться актуальными (действительными);

- достоверность идентификационных данных и подлинность носителей, используемых при документальном подтверждении: при рассмотрении свидетельств необходимо учитывать вероятность наличия ошибок и возможность подделки носителей или фальсификации значений идентификационных атрибутов[1)];

- процесс передачи свидетельств. При анализе свидетельств необходимо учитывать возможность внесения изменений во время передачи, а также возможность отказа от факта предоставления подтверждающей информации.

5.2.5 Для некоторых идентификационных атрибутов в конкретной среде функционирования могут быть доступны официальные свидетельства. Подтверждающая информация в данных свидетельствах, при условии их подлинности и корректности передачи свидетельств, должна рассматриваться как достоверная.

5.2.6 При невозможности или при отсутствии необходимости[2)] использования при подтверждении идентификационных данных официальных свидетельств следует использовать подтверждающие свидетельства.

Примечание — Если подтверждающие свидетельства содержат подтверждающую информацию из общеизвестных официальных свидетельств, то она не может считаться идентичной (равносильной) подтверждающей информации официальных свидетельств.

5.2.7 Реализации процесса первичной идентификации, используемые в конкретных средах функционирования, могут отличаться как требованиями, предъявляемыми к первичной идентификации, так и составом и содержанием свидетельств идентичности.

5.2.8 Получение положительных результатов проверки существования идентификационных данных не означает, что заявленные идентификационные данные действительно соответствуют (принадлежат) субъекту (объекту) доступа или могут быть связаны с ним определенным образом. Для достоверного установления соответствия необходимо осуществить привязку идентификационных данных к субъекту (объекту) доступа. При привязке должны использоваться следующие факторы[3)]:

- фактор знания. Привязка устанавливается с использованием информации, которая известна (свойственна) субъекту (объекту) доступа;

- фактор владения. Привязка устанавливается с использованием идентификационных данных, которые имеет (которыми обладает) субъект (объект) доступа. При этом идентификационные данные могут быть свойственны субъекту (объекту) доступа или содержаться в его свидетельствах, представляющих собой документальное подтверждение. Субъект (объект) доступа должен правомочно обладать данными свидетельствами;

- биометрический фактор. Привязка устанавливается по результатам верификации биометрических характеристик, которые свойственны субъекту доступа — физическому лицу. При этом принимается, что эталонные характеристики субъекта доступа действительно принадлежат ему.

Примечания

1 Условно считается, что при привязке для субъектов доступа и объектов доступа, которые являются информационными и вычислительными ресурсами [средствами вычислительной техники, автоматизированными (информационными) системами и т. п.], используется один фактор. По решению оператора и при выполнении условий, определенных требованиями к первичной идентификации, может считаться, что при привязке субъектов доступа и объектов доступа, которые являются информационными и вычислительными ресурсами, используется более одного фактора.

---

1) Наиболее актуально в отношении свидетельств, представляемых субъектом доступа, ассоциированным с физическим лицом.

2) Если необходимость получения официальных свидетельств не определена требованиями к первичной идентификации.

3) Общая характеристика факторов идентификации — по ГОСТ Р 58833.

2 Привязка с использованием биометрического фактора применяется для субъектов доступа, ассоциированных с физическими лицами. Порядок и правила применения биометрического фактора определяются соответствующими нормативными правовыми документами и документами по стандартизации.

5.3 Уровни доверия первичной идентификации

5.3.1 Уровень доверия первичной идентификации обуславливается уникальностью идентификационных данных и определяется обоснованно подтвержденным соответствием (принадлежностью) заявленных идентификационных данных субъекту (объекту) доступа, которое зависит от результатов проверки существования идентификационных данных и их привязки к субъекту (объекту) доступа.

5.3.2 Устанавливаются три уровня доверия первичной идентификации: низкий, средний, высокий.

На низком уровне доверия первичной идентификации имеется некоторая уверенность в том, что идентификационные данные действительно соответствуют (принадлежат) субъекту (объекту) доступа, который их заявил. При этом идентификационные данные являются уникальными для конкретной среды функционирования, а также предполагается, что идентификационные данные существуют, соответствуют заявленным и предположительно имеют связь с субъектом (объектом) доступа. Регистрация идентификационных данных осуществляется без проверки (верификации), такими, какими их заявляет субъект (объект) доступа.

На среднем уровне доверия первичной идентификации имеется умеренная уверенность в том, что идентификационные данные действительно соответствуют (принадлежат) субъекту (объекту) доступа, который их заявил. При этом идентификационные данные являются уникальными для конкретной среды функционирования, регистрация идентификационных данных осуществляется после их верификации, существование идентификационных атрибутов и достоверность их значений должны удостоверяться подтверждающими свидетельствами, а привязка идентификационных данных к субъекту (объекту) доступа должна выполняться с использованием одного и более факторов.

На высоком уровне доверия первичной идентификации имеется значительная уверенность в том, что идентификационные данные действительно соответствуют (принадлежат) субъекту (объекту) доступа, который их заявил. При этом идентификационные данные являются уникальными для конкретной среды функционирования, регистрация идентификационных данных осуществляется после их верификации, существование идентификационных атрибутов и достоверность их значений должны подтверждаться официальными свидетельствами, а привязка идентификационных данных к субъекту (объекту) доступа должна выполняться с использованием двух и более факторов.

Общая характеристика уровней доверия первичной идентификации приведена в приложении А.

5.3.3 Если существует необходимость достижения среднего или высокого доверия первичной идентификации при недостаточности подтверждающей информации, то могут использоваться вспомогательные атрибуты субъекта (объекта) доступа или должна применяться документированная процедура, определяющая перечень мер, которые позволяют определить существование идентификационных атрибутов и достоверность их значений с уверенностью, соответствующей требуемому уровню доверия.

5.3.4 Если имеется необходимость регистрации субъектов доступа, идентификационные данные которых при первичной идентификации не удовлетворяют необходимому уровню доверия, как минимум, низкому, по причине несоответствия установленным требованиям или недостаточности (отсутствия) подтверждающей информации, то данный субъект доступа определяется как анонимный субъект доступа (аноним). При этом нет никакой уверенности в том, что идентификационные данные действительно соответствуют (принадлежат) субъекту доступа, который их заявил, или в том, что данный субъект доступа существует.

5.4 Общий порядок первичной идентификации

5.4.1 В общем случае первичная идентификация включает:

а) получение регистрирующей стороной запроса на регистрацию субъекта (объекта) доступа;

б) получение от субъекта (объекта) доступа идентификационных данных, требуемых для первичной идентификации. Одновременно от субъекта (объекта) доступа могут быть получены свидетельства, подтверждающие, как минимум, идентификационные данные, наличие которых обязательно для успешной первичной идентификации;

в) установление регистрирующей стороной соответствия между субъектом (объектом) доступа и заявленными им идентификационными данными, в том числе:

1) проверку уникальности идентификационной информации, основанной на заявленных идентификационных данных;
2) сбор подтверждающей информации;
3) проверку существования заявленных идентификационных данных субъекта (объекта) доступа путем их верификации и получения свидетельств от верифицирующей стороны (полномочной верифицирующей стороны);
4) привязку верифицированных идентификационных данных к субъекту (объекту) доступа;
5) принятие решения о соответствии между субъектом (объектом) доступа и заявленными им идентификационными данными;

г) принятие решения регистрирующей стороной о результатах первичной идентификации субъекта (объекта) доступа, в том числе:

1) оценка соответствия уровня доверия, достигнутого при первичной идентификации субъекта (объекта) доступа, уровню доверия, который установлен требованиями к первичной идентификации;
2) формирование идентификационной информации на основе подтвержденных идентификационных данных и назначение идентификатора субъекту (объекту) доступа.

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

3) регистрация идентификационной информации и присвоенного субъекту (объекту) доступа идентификатора или обоснованный отказ в его регистрации.

5.4.2 Регистрирующая сторона в соответствии с требованиями к первичной идентификации должна обеспечить сбор и анализ подтверждающей информации таким образом, чтобы установить и подтвердить соответствие (принадлежность) заявленных идентификационных данных субъекту доступа в соответствии с устанавливаемыми требованиями к первичной идентификации.

5.4.3 Проверка регистрирующей стороной идентификационных данных на уникальность в конкретной среде функционирования должна выполняться, как минимум, для идентификационных атрибутов, обязательность представления которых определена требованиями к первичной идентификации.

5.4.4 Регистрирующая сторона может принять заявленные идентификационные данные (например, на низком уровне доверия первичной идентификации) или провести верификацию идентификационных данных при выявлении несоответствий в них. Верификация заявленных идентификационных данных должна проводиться в обязательном порядке на среднем и высоком уровнях доверия первичной идентификации.

Регистрирующая сторона может выполнять верификацию самостоятельно и/или может использовать услуги верифицирующей стороны.

Примечание — В качестве верифицирующей стороны может рассматриваться субъект (объект) доступа, если он имеет возможность представить свидетельство идентичности.

Ответ верифицирующей стороны может представлять собой:

- свидетельство идентичности, содержащее верифицированные идентификационные данные или верифицированную подтверждающую информацию для идентификационных данных;
- подтверждающую информацию, в том числе из источников данных, которая может быть использована регистрирующей стороной для установления соответствия между субъектом (объектом) доступа и заявленными им идентификационными данными.

5.4.5 При получении ответа регистрирующая сторона полагается на точность и достоверность полученной подтверждающей информации, но при необходимости может выполнить верификацию заявленных идентификационных данных и у другой верифицирующей стороны. Регистрирующая сторона может использовать любое количество свидетельств, которое необходимо для подтверждения идентификационных данных.

Примечание — При большом количестве свидетельств можно достигнуть большей уверенности, применяя свидетельства, относящиеся ко всему периоду существования субъекта (объекта) доступа.

5.4.6 В процессе передачи подтверждающей информации между верифицирующей и регистрирующей стороной должны быть реализованы меры, обеспечивающие ее конфиденциальность и целостность, а также неизменность свидетельств и неотказуемость от внесенной в них подтверждающей информации. Кроме того, при рассмотрении свидетельств, полученных регистрирующей стороной на

носителях, должны проверяться присущие носителям признаки защиты от подделки, а также учитываться процессы, используемые для их выпуска.

5.4.7 Привязка заявленных идентификационных данных к субъекту доступа, который является физическим лицом, должна выполняться при его личном контакте с регистрирующей стороной. Биометрический фактор должен использоваться только совместно с другими факторами, в том числе для подтверждения фактора владения. Применение биометрического фактора в качестве единственного фактора привязки не допускается.

Примечание — Условия (правила) привязки заявленных идентификационных данных к субъекту доступа, который является физическим лицом, могут быть изменены в случаях, определенных нормативными правовыми актами, документами по стандартизации или в случаях, определенных оператором для конкретной среды функционирования в требованиях к первичной идентификации.

Подтверждающая информация, полученная в результате привязки от субъекта (объекта) доступа, при необходимости, должна быть верифицирована регистрирующей стороной относительно свидетельств, полученных от верифицирующей стороны, либо направлена ей на верификацию.

5.4.8 Уровень доверия первичной идентификации должен определяться на основе подтверждающей информации, которая соответствует требованиям к первичной идентификации и обоснованно удостоверяет (доказывает) соответствие (принадлежность) заявленных идентификационных данных субъекту (объекту) доступа.

На основе результатов оценки соответствия достигнутого уровня доверия уровню доверия, который установлен требованиями к первичной идентификации, регистрирующей стороной принимается решение о регистрации идентификационной информации, сформированной на основе подтвержденных идентификационных данных, о присвоении и регистрации идентификатора субъекта (объекта) доступа в перечне(ях) идентификаторов доступа, или решение об обоснованном отказе в регистрации.

6 Вторичная идентификация

6.1 Целью вторичной идентификации является опознавание субъекта доступа, запросившего доступ к объекту доступа.

6.2 Вторичная идентификация заключается в проверке наличия идентификатора доступа, предъявленного субъектом доступа, в перечне идентификаторов, присвоенных субъектам (объектам) доступа при первичной идентификации. Проверка наличия идентификатора доступа осуществляется по предопределенному алгоритму и может выполняться в том числе путем сравнения.

6.3 Положительный результат вторичной идентификации субъекта доступа обеспечивает связывание идентификатора доступа субъекта доступа с идентификационной информацией и, после его успешной аутентификации, позволяет однозначно определить субъекта доступа, который должен быть впоследствии авторизован.

Примечания

1 Аутентификация субъекта доступа осуществляется после его вторичной идентификации.

2 Порядок и правила аутентификации определяются соответствующими нормативными правовыми актами и документами по стандартизации.

7 Уровни доверия идентификации

7.1 Уровень доверия идентификации определяется уровнем доверия первичной идентификации и зависит от результатов вторичной идентификации.

7.2 Устанавливаются три уровня доверия идентификации:

- низкий уровень доверия. На данном уровне доверия идентификации имеется некоторая уверенность в том, что субъект доступа, успешно прошедший идентификацию, действительно соответствует зарегистрированной идентификационной информации, которая однозначно определяется соотнесенным с ней предъявленным идентификатором доступа. Низкий уровень доверия идентификации соответствует низкому уровню доверия первичной идентификации при условии успешной вторичной идентификации;

- средний уровень доверия. На данном уровне доверия идентификации появляется умеренная уверенность в том, что субъект доступа, успешно прошедший идентификацию, действительно соответ-

ствует зарегистрированной идентификационной информации, которая однозначно определяется соотнесенным с ней предъявленным идентификатором доступа. Средний уровень доверия идентификации соответствует среднему уровню доверия первичной идентификации при условии успешной вторичной идентификации;

- высокий уровень доверия. На данном уровне доверия идентификации существует значительная уверенность в том, что субъект доступа, успешно прошедший идентификацию, действительно соответствует зарегистрированной идентификационной информации, которая однозначно определяется соотнесенным с ней предъявленным идентификатором доступа. Высокий уровень доверия идентификации соответствует высокому уровню доверия первичной идентификации при условии успешной вторичной идентификации.

Общая характеристика уровней доверия идентификации приведена в приложении А.

7.3 Уровень доверия идентификации, который необходимо реализовать в конкретной среде функционирования, должен устанавливаться в соответствии с нормативными правовыми документами и/или на основе результатов анализа рисков информационной безопасности, выполняемого в соответствии с ГОСТ Р ИСО/МЭК 27005, а также с учетом положений ГОСТ Р 58833.

Приложение А
(справочное)

Общая характеристика уровней доверия первичной идентификации

Возможность регистрации субъекта (объекта) доступа и уровень доверия, достигаемый при первичной идентификации, обусловливается уникальностью идентификационных данных и зависит от результатов проверки существования идентификационных данных и привязки идентификационных данных к субъекту (объекту) доступа.

Таблица А.1 — Общая характеристика уровней доверия первичной идентификации

Первичная регистрация субъекта (объекта) доступа			Необходимость подтверждения идентификационных данных	Уверенность в том, что субъект (объект) доступа действительно соответствует заявленным идентификационным данным	Уровень доверия первичной идентификации	Возможность регистрации субъекта (объекта) доступа
Уникальность идентификационной информации	Подтверждение идентификационных данных					
	Существование идентификационных данных	Привязка идентификационных данных				
Заявленные идентификационные данные не соответствуют требованиям к первичной идентификации			Не рассматривается	Не рассматривается	Не рассматривается	Отказ в регистрации субъекта (объекта) доступа
Заявленные идентификационные данные не соответствуют требованиям к первичной идентификации			Отсутствует необходимость подтверждения	Нет уверенности	Не достигнут низкий уровень доверия	Регистрация субъекта доступа как анонима
Уникальность обеспечивается	Существование не проверяется	Привязка не выполняется	Необходимо подтверждение	Некоторая уверенность	Низкий уровень доверия	Регистрация субъекта (объекта) доступа
Уникальность обеспечивается	Существование заверяется подтверждающими свидетельствами	Привязка с использованием одного фактора	Необходимо подтверждение	Умеренная уверенность	Средний уровень доверия	Регистрация субъекта (объекта) доступа
Уникальность обеспечивается	Существование подтверждается официальными свидетельствами	Привязка с использованием двух и более факторов	Необходимо подтверждение	Значительная уверенность	Высокий уровень доверия	Регистрация субъекта (объекта) доступа

Библиография

1] NIST.SP.800-63-3 Руководства по цифровым идентификационным данным (Digital Identity Guidelines)

[2] NIST.SP.800-63A Руководства по цифровым идентификационным данным. Регистрация и подтверждение идентификационных данных (Digital Identity Guidelines. Enrollment and Identity Proofing)

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

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

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

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

УДК 004:006.354 ОКС 35.030

Ключевые слова: защита информации, идентификация, уровень доверия идентификации, управление доступом, первичная идентификация, вторичная идентификация, идентификационные данные, идентификационные атрибуты, идентификационная информация

Редактор *Л.В. Коретникова*
Технический редактор *И.Е. Черепкова*
Корректор *М.И. Першина*
Компьютерная верстка *М.В. Малеевой*

Сдано в набор 08.08.2022. Подписано в печать 10.08.2022. Формат 60×84⅛. Гарнитура Ариал.
Усл. печ. л. 2,79. Уч.-изд. л. 2,51.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

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