ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р

(проект, первая редакция)

Защита информации

ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ

Уровни доверия к результатам идентификации

Настоящий проект стандарта не подлежит применению до его утверждения

20XX

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)

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.

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. Фундаментом 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 ресурсам средств вычислительной техники. Данное соответствие, как правило, устанавливается при регистрации ресурса как объекта 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, имеющего на это соответствующие права.

При подготовке настоящего стандарта учитывались нормы, определенные базовым документом в области идентификации и аутентифи-

кации – национальным стандартом ГОСТ Р «Идентификация и аутентификация. Общие положения», а также правила идентификации, установленные международными и зарубежными стандартами в данной области [1, 2, 3, 4].

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

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Защита информации

ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ

Уровни доверия к результатам идентификации

Information protection. Identification and authentication.
Identification Results Assurance Levels

Дата введения — _____

1 Область применения

Настоящий стандарт устанавливает единообразную организацию процесса идентификации субъектов и объектов доступа в средствах защиты информации, в том числе реализующих криптографическую защиту, средствах вычислительной техники и автоматизированных (информационных) системах, а также определяет общие правила 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 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 Р 50922–2006 Защита информации. Основные термины и определения

ГОСТ Р Защита информации. Идентификация и аутентификация. Общие положения

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 (сводов правил и/или классификаторов) в информационной системе общего пользования - на официальном сайте федерального органа исполнительной власти в сфере стандартизации в сети Интернет или по ежегодно издаваемому информационному указателю «Национальные стандарты», который опубликован по состоянию на 1 января текущего года, и по выпускам ежемесячно издаваемого информационного указателя «Национальные стандарты» за текущий год. Если заменен ссылочный стандарт (документ), на который дана недатированная ссылка, то рекомендуется использовать действующую версию этого стандарта (документа) с учетом всех внесенных в данную версию изменений. Если заменен ссылочный стандарт (документ), на который дана датированная ссылка, то рекомендуется использовать версию этого стандарта (документа)

с указанным выше годом утверждения (принятия). Если после утверждения настоящего стандарта в ссылочный стандарт (документ), 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 (документ) 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, 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 Идентификация и аутентификация. Общие положения, пункт 3.1]

3.2

атрибут: Признак или свойство субъекта доступа или объекта доступа.

[ГОСТ Р Идентификация и аутентификация. Общие положения, пункт 3.2]

3.3

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

[ГОСТ Р Идентификация и аутентификация. Общие положения, пункт 3.9]

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

3.5 **вспомогательный атрибут**: 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.

3.6

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 Идентификация и аутентификация. Общие положения, пункт 3.12]

3.7

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]

3.8

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, рассматриваются в качестве оснований для уверенности.

3.9

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 [2].

[ГОСТ Р Идентификация и аутентификация. Общие положения, пункт 3.17]

3.10

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 Идентификация и аутентификация. Общие положения, пункт 3.20]

3.11

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

[ГОСТ Р Идентификация и аутентификация. Общие положения, пункт 3.21]

3.12

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

[ГОСТ Р Идентификация и аутентификация. Общие положения, пункт 3.22]

Примечание – Идентификационные данные, которые подтверждены в соответствии с установленными требованиям к первичной идентификации, считаются подтвержденными идентификационными данными.

3.13

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

[ГОСТ Р Идентификация и аутентификация. Общие положения, пункт 3.23]

3.14

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]

3.15

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]

3.16

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

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

3.17 **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 [5].

3.18

объект доступа: Одна из сторон информационного взаимодействия, которая предоставляет доступ.

[ГОСТ Р Идентификация и аутентификация. Общие положения, пункт 3.33]

3.19

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]

3.20 **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 [5].

3.21 **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.

3.22

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 Идентификация и аутентификация. Общие положения, пункт 3.41]

3.23

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

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

3.24

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

[ГОСТ Р Идентификация и аутентификация. Общие положения, пункт 3.43]

Примечание – Подтверждающая информация собирается в рамках обеспечения доверия и рассматривается в качестве оснований для уверенности в результатах первичной идентификации.

3.25 **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.

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

Примечание – Адаптировано из ГОСТ Р 53114-2008.

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

Примечания

1 К управлению идентификационными атрибутами (значениями идентификационных атрибутов) относится, например, их создание, изменение, удаление, выпуск, отзыв, верификация, подтверждение и т.п.

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.

3.28

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

Примечания

1 Адаптировано из Р 50.1.053-2005.

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

3 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.

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

[ГОСТ Р Идентификация и аутентификация. Общие положения, пункт 3.45]

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

3.30

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

Примечание – Процедуры могут быть документированными или нет.

[ГОСТ Р ИСО 9000-2015, пункт 3.4.5]

3.31

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

[ГОСТ Р ИСО 9000-2015, пункт 3.4.1]

3.32

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]

3.33

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

[ГОСТ Р Идентификация и аутентификация. Общие положения, пункт 3.50]

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

Примечание – В качестве свидетельств идентичности могут рассматриваться, например, результаты верификации заявленных идентификационных данных, документальные подтверждения (официальные документы), представленные субъектом доступа, а также другая подтверждающая информация.

3.35

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 Идентификация и аутентификация. Общие положения, пункт 3.53]

3.36

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

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

[ГОСТ Р Идентификация и аутентификация. Общие положения, пункт 3.55]

3.37

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]

3.38

управление доступом: Предоставление санкционированного и предотвращение несанкционированного доступа.

[ГОСТ Р Идентификация и аутентификация. Общие положения, пункт 3.57]

3.39

уровень доверия: 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 формированию и регистрации идентификационной информации субъекта (объекта) доступа, а также присвоению и регистрации идентификатора субъекта (объекта) доступа в перечне идентификаторов доступа, а при доступе субъекта доступа к объекту доступа – действия по проверке существования (наличия) идентификатора, предъявленного субъектом доступа, в перечне (перечнях) идентификаторов, присвоенных субъектам (объектам) доступа.

4.2 В общем случае идентификация, с учетом особенностей, определенных ГОСТ Р «Идентификация и аутентификация. Общие положения», должна включать:

- первичную идентификацию субъекта (объекта) доступа, которая охватывает распознавание субъекта (объекта) доступа по заявленным

им идентификационным данным, формирование идентификационной информации и присвоение идентификатора доступа субъекту (объекту) доступа, а также 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 «Идентификация и аутентификация. Общие положения». 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.

4.4 Участники процесса идентификации должны обеспечивать защиту информации, используемой при идентификации. При этом состав и

содержание мер защиты в конкретной среде функционирования информации должны определяться оператором 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 документа в конкретной среде функционирования.

4.6 Уверенность в результатах идентификации для конкретной среды функционирования обеспечивается доверием к 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 конкретной среды функционирования. При необходимости, в конкретной среде функционирования, субъект (объект) до-

ступа 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, установленными 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; 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.

5.1.4 Требования к первичной идентификации должны содержать:

- уровень доверия, который необходимо достигнуть при первичной идентификации;

- характеристику среды функционирования, для которой осуществляется первичная идентификация субъекта доступа и результаты 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 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;

- порядок сбора подтверждающей информации и действия регистрирующей стороны при ее недостаточности;

- порядок и правила верификации заявленных идентификационных данных или идентификационной информации, полученной из свидетельств, представленных (имеющихся) субъектом (объектом) 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;

- возможность и порядок регистрации субъектов доступа, идентификационные данные которых не соответствуют установленным требованиям.

5.1.5 Требования к первичной идентификации субъектов (объектов) доступа должны устанавливаться обладателем информации или оператором на основе положений нормативных правовых актов, норма-

тивных документов и документов по стандартизации с учетом особенностей конкретной среды функционирования. При этом состав и строгость требований должны обеспечить первичную идентификацию субъекта (объекта) доступа с уверенностью, необходимой в данной среде функционирования.

Примечание – Требования к первичной идентификации субъектов (объектов) доступа могут оформляться в виде отдельных документированных процедур (политик) и/или могут включаться в политику информационной безопасности организации.

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

5.1.7 При первичной идентификации должна выполняться проверка уникальности значений отдельных идентификационных атрибутов, либо 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 единожды, 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 или их значения, которые 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 в конкретной среде функционирования должны использоваться подтвержденные идентификационные данные субъекта (объекта) доступа. В процессе подтверждения необходимо осуществить проверку существования (верификацию) заявленных идентификационных данных 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 действительно 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.

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.

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

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 должны использоваться свидетельства, базирующиеся на реальных 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 должны использоваться подтверждающие свидетельства.

Примечание – Если подтверждающие свидетельства содержат подтверждающую информацию из 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.

[1)] В наибольшей степени актуально в отношении свидетельств, представляемых субъектом доступа, ассоциированным с физическим лицом.

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

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 этом должны использоваться механизмы привязки с использованием следующих факторов[1)]:

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

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

- фактор биометрический. Привязка устанавливается по результатам верификации биометрических характеристик, которые свойственны субъекту доступа. 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, при выполнении условий, определенных требованиями к первичной идентификации, может считать-

---

[1)] Общая характеристика факторов – по ГОСТ Р Идентификация и аутентификация. Общие положения.

ся, что при привязке субъектов доступа и объектов доступа, которые являются информационными и вычислительными ресурсами, используется более одного фактора.

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

5.2.9 Уровень подтверждения идентификационных данных определяется существованием идентификационных данных, а также привязкой идентификационных данных к субъекту (объекту) доступа.

5.2.10 Устанавливается три уровня подтверждения идентификационных данных: низкий, средний, высокий.

На низком уровне подтверждения 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 подтверждения регистрация идентификационных данных осуществляется после их верификации, при этом 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 подтверждения 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.

5.2.11 Если существует необходимость достижения среднего или высокого уровня подтверждения при недостаточности подтверждающей информации, то могут использоваться вспомогательные атрибуты субъекта доступа или должна применяться документированная процедура, определяющая перечень мер, которые позволяют определить существование идентификационных атрибутов и достоверность их значений с достаточной уверенностью. Данные меры должны быть пропорциональны требуемому уровню подтверждения.

5.3 Уровни доверия к результатам первичной идентификации

5.3.1 Уровень доверия к результатам первичной идентификации обусловливается уникальностью идентификационных данных и определяется уровнем их подтверждения.

5.3.2 Устанавливается три уровня доверия к результатам первичной идентификации: низкий, средний, высокий.

На низком уровне доверия к результатам 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 и достигнут низкий уровень их подтверждения.

На среднем уровне доверия к результатам 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 и обеспечен средний уровень их подтверждения.

На высоком уровне доверия к результатам 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 и обеспечен высокий уровень их подтверждения.

5.3.3 Если имеется необходимость регистрации субъектов доступа, идентификационные данные которых не могут обеспечить достижение низкого уровня доверия к первичной идентификации по причине несоответствия установленным требованиями или отсутствия подтверждающей информации, то данный субъект доступа определяется как анонимный субъект доступа («аноним») и нет никакой уверенности в том, что идентификационные данные действительно соответствуют (принадлежат) субъекту доступа, который их заявил, или в том, что данный субъекту доступа существует.

Общая характеристика уровней доверия к результатам первичной идентификации приведена в приложении А.

5.4 Общий порядок первичной идентификации

5.4.1 В процессе первичной идентификации взаимодействуют субъект доступа и регистрирующая сторона, а также следующие дополнительные участники, которые имеют функциональные возможности (роли), обусловленные особенностями процесса первичной идентификации:

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

- полномочная верифицирующая сторона (полномочная сторона). Основной задачей полномочной стороны является управление идентификационными данными, в том числе и верификация по запросам реги-

стрирующей стороны заявленных идентификационных данных субъекта доступа и их подтверждение официальными свидетельствами.

5.4.2 В общем случае первичная идентификация включает:

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

б) предоставление физическим лицом или получение от ресурса идентификационных данных, требуемых для первичной идентификации. Одновременно субъект (объект) доступа может предоставить свидетельства, подтверждающие, как минимум, идентификационные данные, наличие которых обязательно для успешной первичной идентификации;

в) подтверждение соответствия между заявленными идентификационными данными и субъектом (объектом) доступа регистрирующей стороной, а также оценка возможности регистрации субъекта (объекта) доступа, включая:

1) формирование идентификационной информации на основе заявленных идентификационных данных субъекта (объекта) доступа и проверка ее уникальности;

2) сбор регистрирующей стороной подтверждающей информации;

3) проверка существования заявленных идентификационных данных субъекта (объекта) доступа путем их верификации и получения свидетельств от верифицирующей стороны (полномочной верифицирующей стороны);

4) привязка регистрирующей стороной верифицированных идентификационных данных к субъекту (объекту) доступа;

5) определение уровня подтверждения идентификационных данных;

6) оценка достигнутого уровня доверия к результатам первичной идентификации субъекта доступа и соотнесение его с уровнем, которого необходимо достигнуть в конкретной среде функционирования.

г) принятие решения регистрирующей стороной о результатах первичной идентификации субъекта (объекта) доступа, в том числе регистрация идентификационной информации и присвоенного субъекту (объекту) доступа идентификатора или обоснованный отказ в регистрации.

5.4.3 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 и обеспечить достижение необходимого уровня их подтверждения.

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.

Регистрирующая сторона может принять заявленные идентификационные данные (на низком уровне доверия к результатам 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 к результатам первичной идентификации.

Верификация может выполняться регистрирующей стороной и/или могут использоваться 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 как свидетельство идентичности, содержащее верифицированные идентификационные данные или подтверждения для идентификационных данных, так и представлять собой подтверждающую информацию, которая может быть использована регистрирующей стороной для установления соответствия между субъектом (объектом) доступа и заявленными им идентификационными данными. При этом 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 достижения требуемого уровня подтверждения идентификационных данных.

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

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 процесс, используемый для их выпуска.

Привязка заявленных идентификационных данных к субъекту доступа, который является физическим лицом, должна выполняться в условиях его личного контакта с регистрирующей стороной. Фактор био-

метрический должен использоваться только совместно с другими факторами, в том числе для подтверждения фактора владения. Применение фактора биометрического 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.

Оценка уровня доверия к результатам первичной идентификации должна выполняться на основе подтверждающей информации, которая соответствует требованиям к первичной идентификации и подтверждает соответствие (принадлежность) заявленных идентификационных данных субъекту (объекту) доступа с необходимой уверенностью.

На основе результатов оценки уровня доверия, достигнутого в процессе первичной идентификации субъекта (объекта) доступа, регистрирующей стороной принимается решение о его регистрации в перечне субъектов (объектов) доступа или субъекту (объекту) доступа обоснованно отказывается 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 существо-

вания (наличия) идентификатора доступа, предъявленного субъектом доступа, в перечне идентификаторов, присвоенных субъектам (объектам) доступа при первичной идентификации. Проверка существования (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, что, после его успешной аутентификации, позволяет однозначно определить субъекта доступа, который должен быть впоследствии авторизован.

Примечание

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 к результатам идентификации

7.1 Уровень доверия к результатам идентификации определяется уровнем доверия к результатам первичной идентификации и зависит от результатов вторичной идентификации. Уровень доверия обусловливает степень достижения целей идентификации.

7.2 Устанавливается три уровня доверия к результатам идентификации:

- низкий уровень доверия. На данном уровне доверия к результатам идентификации существует 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 к результатам иден-

тификации соответствует низкому уровню доверия к результатам первичной идентификации при условии успешной вторичной идентификации;

- средний уровень доверия. На данном уровне доверия к результатам идентификации существует умеренная уверенность в том, что субъект доступа, успешно прошедший идентификацию, действительно соответствует зарегистрированной идентификационной информации, которая однозначно определяется соотнесенным с ней предъявленным идентификатором доступа. Средний уровень доверия к результатам идентификации соответствует среднему уровню доверия к результатам первичной идентификации при условии успешной вторичной идентификации;

- высокий уровень доверия. На данном уровне доверия к результатам 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 к результатам идентификации соответствует высокому уровню доверия к результатам первичной идентификации при условии успешной вторичной идентификации.

7.3 Уровень доверия к результатам идентификации, который должен быть достигнут 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 27005-2010, а также с учетом положений ГОСТ Р «Защита информации. Идентификация и аутентификация. Общие положения.

Приложение А

(справочное)

Общая характеристика уровней доверия к результатам первичной идентификации

Возможность регистрации субъекта (объекта) доступа и уровень доверия, достигнутый при первичной идентификации, обусловливается уникальностью идентификационных данных и определяется уровнем подтверждения соответствия субъекта (объекта) доступа заявленным идентификационным данным, который зависит от результатов проверки существования идентификационных данных и привязки идентификационных данных к субъекту (объекту) доступа

Таблица А.1 – Общая характеристика уровней доверия к результатам первичной идентификации

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

Библиография

[1] ISO/IEC TS 29003:2018 Информационная технология – Методы и средства обеспечения безопасности – Подтверждение идентификационных данных (Information technology – Security techniques – Identity proofing)

[2] ISO/IEC 24760-2:2015 Информационная технология – Методы и средства обеспечения безопасности – Основы управления идентификацией – Часть 2 – Базовая архитектура и требования (Information technology – Security techniques -- A framework for identity management – Part 2: Reference architecture and requirements)

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

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

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

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

УДК 004 ОКС 35.030

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