ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р

(проект, первая редакция)

Защита информации

ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ

Рекомендации по управлению идентификацией и аутентификацией

Настоящий проект стандарта не подлежит применению до его утверждения

Москва
Российский институт стандартизации

202_

ГОСТ Р
(проект, первая редакция)

Предисловие

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

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 «___» _____ 20__ № _____

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 (www.rst.gov.ru)

ГОСТ Р
(проект, первая редакция)

Содержание

ГОСТ Р
(проект, первая редакция)

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 определенному физическому лицу и конкретному информационному 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, к которым осуществляется доступ. Данное соответствие, как правило, устанавливается при регистрации ресурса как объекта или субъекта доступа и физического лица как пользователя (субъекта доступа), проверяется при опознавании субъекта доступа по предъявленному идентификатору доступа, подтверждается при проверке его подлинности и обеспечивает определенную уверенность в том, что обработка данных вычислительными процессами действительно инициирована физическим лицом или ресурсом, имеющим на это право. С целью поддержания актуальности, правильности, достоверности и регламентации использования инфор-

мации (данных), которая применяется при принятии решений о возможности регистрации объекта (субъекта) доступа, соответствии между субъектом доступа и предъявленным идентификатором при идентификации и подлинности субъекта (объекта) при аутентификации, необходимо осуществлять управление идентификацией и аутентификацией. Управление, осуществляется в рамках структуры управления, обеспечивающей формирование, администрирование и использование идентификационной и аутентификационной информации. При формировании данной структуры следует определить правила взаимодействия для сторон, участвующих в идентификации и аутентификации, а также реализовать защиту используемой информации (данных).

При подготовке настоящего стандарта учитывались нормы, установленные ГОСТ Р 58833, ГОСТ Р 70262.1, ГОСТ ISO/IEC 24760-2, а также правила, определенные [1 – 5].

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

ГОСТ Р
(проект, первая редакция)

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Защита информации

ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ

Рекомендации по управлению идентификацией и аутентификацией

Information protection. Identification and authentication.
Recommendations for
identity and authentication management

Дата введения — _____

1 Область применения

Настоящий стандарт определяет базовый состав структуры, обеспечивающей формирование, администрирование и использование идентификационной и аутентификационной информации, рекомендуемые правила взаимодействия для сторон, участвующих в идентификации и аутентификации, а также меры защиты используемой информации (данных).

Положения настоящего стандарта могут использоваться для реализации требований ГОСТ Р «Защита информации. Идентификация и аутентификация. Управление идентификацией и аутентификацией» (проект), а также при планировании, проектировании и реализации процедур управления доступом к информационным ресурсам, вычислительным ресурсам средств вычислительной техники, ресурсам автоматизированных, информационных и других систем, средствам вычислительной техники и автоматизированным, информационным и другим си-

стемам 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 70262.1 Защита информации. Идентификация и аутентификация. Уровни доверия идентификации

ГОСТ Р Защита информации. Идентификация и аутентификация. Уровни доверия аутентификации (проект)

ГОСТ Р Защита информации. Идентификация и аутентификация. Управление идентификацией и аутентификацией (проект)

Примечание – При пользовании настоящим стандартом целесообразно проверить действие ссылочных стандартов в информационной системе общего пользования – на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет или по ежегодному информационному указателю «Национальные стандарты», который опубликован по состоянию на 1 января текущего года, и по выпускам ежемесячного информационного указателя «Национальные стандарты» за текущий год. Если заменен ссылочный стандарт, на который дана недатированная ссылка, то рекомендуется использовать действующую версию этого стандарта с учетом всех внесенных в данную версию изменений. Если заменен ссылочный стандарт, на который дана датированная ссылка, то рекомендуется использовать версию этого стандарта с указанным выше годом утверждения (принятия). Если после утверждения настоящего стандарта в ссылочный стандарт, на который дана датированная ссылка, внесено изменение, затрагивающее положение, на которое дана ссылка, то это положение рекомендуется применять без учета данного изменения. Если ссылочный стандарт отменен без замены, то положение, в котором дана ссылка на него, рекомендуется применять в части, не затрагивающей эту ссылку.

3 Термины и определения

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

3.1

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

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

3.2

аутентификатор: аутентификационная информация (и другие данные, необходимые при аутентификации) и устройство аутентификации (при записи аутентификационной информации в устройство аутентификации), ассоциированные с субъектом (объектом) доступа, которые

назначаются при регистрации и используются для аутентификации субъекта (объекта) доступа.

[Адаптировано из ГОСТ Р Защита информации. Идентификация и аутентификация. Уровни доверия аутентификации (проект), пункт 3.3]

3.3

аутентификационное утверждение: Сообщение протокола аутентификации от проверяющей стороны доверяющей стороне, которое содержит информацию, связанную с доказывающей стороной, подтверждающую ее подлинность.

[ГОСТ Р Защита информации. Идентификация и аутентификация. Уровни доверия аутентификации (проект), пункт 3.4].

3.4

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]

3.5

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

[ГОСТ Р 58833–2020, пункт 3.9]

3.6

верифицирующая сторона: Сторона, которая осуществляет верификацию идентификационных данных.

[ГОСТ Р 70262.1–2022, пункт 3.5]

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 **вторичный аутентификатор:** Временный секрет, выданный проверяющей стороной успешно аутентифицированной доказывающей стороне как часть аутентификационного утверждения.

Примечания

1 Вторичный аутентификатор впоследствии используется доказывающей стороной для аутентификации у доверяющей стороны.

2 Примерами вторичных аутентификаторов являются сеансовые ключи Kerberos.

3.9

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

[ГОСТ 28195–89, приложение 1]

3.10

достоверные идентификационные данные (информация): идентификационные (-ая) данные (информация) сущности (субъекта или объекта доступа), описывающие (соответствующие) реальное состояние ее идентификационных атрибутов на определенный момент времени.

Примечание – Как правило, достоверные идентификационные данные (информация) не содержат ошибок.

[ГОСТ Р Защита информации. Идентификация и аутентификация. Угрозы и уязвимости процессов идентификации и аутентификации (проект), пункт 3.13]

3.11

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

ГОСТ Р
(проект, первая редакция)

Примечания

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

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

[ГОСТ Р 58833–2020, пункт 3.17]

3.12

идентичность: Представление (образ) сущности в виде одного или нескольких атрибутов, которые позволяют сущностям быть различимыми в домене.

[ГОСТ Р 59381—2021, пункт 3.13]

Примечания

1 Как правило идентичность характеризуется совокупностью идентификационных данных.

2 Идентичность может представлять собой идентификационную информацию, подлежащую обработке и/или хранению, которая используются для представления сущности в средствах вычислительной техники и/или автоматизированной, информационной или другой системе.

3.13

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

[ГОСТ Р 58833–2020, пункт 3.20]

3.14

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

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

[ГОСТ Р 70262.1–2022, пункт 3.12]

3.15

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]

3.16

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

[ГОСТ Р 58833–2020, пункт 3.23]

3.17

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

[[6], статья 3.3.9]

ГОСТ Р
(проект, первая редакция)

3.18

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]

3.19

нарушитель (безопасности информации): Активная сущность, совершившая или совершающая действия, следствием которых является или может являться нарушение безопасности информации.

[Адаптировано из ГОСТ Р 53114-2008, статья 3.3.5]

3.20

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.

[[7], статья 2]

3.21

объект доступа: Одна из сторон информационного взаимодействия, предоставляющая доступ или к которой предоставляется доступ внешним по отношению к стороне информационного взаимодействия средством управления доступом.

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

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

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.

[ГОСТ Р 58833-2020, пункт 3.38]

3.23

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]

3.24

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

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

3.25

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]

ГОСТ Р
(проект, первая редакция)

3.26

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]

3.27

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

Примечание – Процедуры могут быть документированными или нет.

[ГОСТ Р ИСО 9000–2015, пункт 3.4.5]

3.28

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

[ГОСТ Р ИСО 9000–2015, пункт 3.4.1]

3.29

протокол идентификации (аутентификации): Коммуникационный протокол, позволяющий участникам осуществлять идентификацию и аутентификацию.

Примечание – Протокол идентификации и/или аутентификации реализует алгоритм (правила), в рамках которого участники процессов идентификации и аутен-

тификации последовательно выполняют определенные действия и обмениваются сообщениями.

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

3.30

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

[[8], пункт А.20]

3.31

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]

3.32

свидетельство идентичности: Объективное доказательство, обеспечивающее уверенность в том, что идентичность действительно соответствует (принадлежит) сущности.

[Адаптировано из ГОСТ Р 70262.1, пункт 3.36]

3.33 **система управления идентификацией и аутентификацией**: Совокупность взаимодействующих (действующих) сущностей (сторон) структуры управления идентификацией и аутентификацией, осуществляющих управление идентификацией и аутентификацией, путем применения (реализации) политик, процедур, технологий, технических средств и других ресурсов для поддержания актуальности идентификационной и аутентификационной информации и осуществления идентификации и аутентификации.

ГОСТ Р
(проект, первая редакция)

3.34

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]

3.35

структура управления идентификацией и аутентификацией: Совокупность органов управления, объектов управления, других участников и взаимосвязей между ними, а также политик и процедур, используемых для управления идентификацией и аутентификацией.

Примечания

1 Органами управления являются сущности (сущность), отвечающие за организацию и поддержание деятельности участников структуры управления посредством создания, организации выполнения и контроля выполнения политик и процедур управления идентификацией и аутентификацией.

2 Объектами управления идентификацией и аутентификацией являются сущности (сущность), отвечающие за реализацию политик и процедур структуры управления идентификацией и аутентификацией.

3 К другим участникам структуры управления идентификацией и аутентификацией относятся, например, сущности, осуществляющие надзор и/или аудит соответствия политик и процедур правовым и нормативным требованиям.

[ГОСТ Р Защита информации. Идентификация и аутентификация. Управление идентификацией и аутентификацией (проект), пункт 3.34]

3.36

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

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

[ГОСТ Р 58833–2020, пункт 3.55]

3.37

сущность: Идентифицируемый (распознаваемый) элемент, который описывается набором свойств.

Примечание – Сущность может иметь различное физическое (реальное) представление. Например, сущность может представлять собой физическое лицо, организацию, ресурс, субъект, объект, информацию и т.п.

[Адаптировано из ISO/IEC 15408-1:2022, пункт 3.36]

3.38

управление доступом: Предоставление санкционированного и предотвращение несанкционированного доступа.

[ГОСТ Р 58833–2020, пункт 3.57]

3.39

управление идентификацией и аутентификацией: Реализация совокупности процессов и политик, связанных с управлением идентификационной и аутентификационной информацией на всех этапах ее жизненного цикла, а также связанных с формированием политик управления доступом и регулированием взаимодействия участников структуры управления идентификацией и аутентификацией.

Примечание – К процессам управления идентификационной и аутентификационной информацией относятся: управление представлением идентификационных данных, управление обработкой и управление предоставлением идентификационной и аутентификационной информации для идентификации и аутентификации.

[ГОСТ Р Защита информации. Идентификация и аутентификация. Управление идентификацией и аутентификацией (проект), пункт 3.40]

ГОСТ Р
(проект, первая редакция)

3.40

уязвимость: Недостаток (слабость, несоответствие) процесса и/или его составной части, который (-ая) может быть использован (-а) для осуществления угроз процессам идентификации и аутентификации.

[Адаптировано из ГОСТ Р 56546-2015, пункт 3.7]

3.41

электронное удостоверение: Совокупность идентификационной информации и аутентификационной информации (или прямого указания ее существования) субъекта доступа или объекта доступа, подлинность которой подтверждена проверяющей стороной.

Примечание – Электронное удостоверение может представлять собой: в простейшем случае идентификатор доступа и пароль; в других случаях – совокупность идентификатора доступа, открытого ключа и другой информации.

[Адаптировано из ГОСТ Р 58833-2020, пункт 3.62]

Примечание – Проверяющей стороной, как правило, является сущность, обладающая на законных основаниях правом предоставления аутентификационных утверждений.

4 Общие положения

4.1 В соответствии с ГОСТ Р 58833, ГОСТ Р 70262.1, ГОСТ Р «Защита информации. Идентификация и аутентификация. Уровни доверия аутентификации» (проект), ГОСТ Р «Защита информации. Идентификация и аутентификация. Управление идентификацией и аутентификацией» (проект), процессы идентификации и аутентификации включают:

- первичную идентификацию субъекта (объекта) доступа, которая обеспечивает распознавание субъекта (объекта) доступа, формирование идентификационной информации на основе подтвержденных идентификационных данных, присвоение идентификатора доступа субъекту

(объекту) доступа и их регистрацию;

Примечание – Состав и содержание процесса первичной идентификации, включая действия, выполняемые участниками процесса, приведены в ГОСТ Р 58833, ГОСТ Р 70262.1 и ГОСТ Р 59515;

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

Примечание – Состав и содержание процесса вторичной идентификации, включая действия, выполняемые участниками процесса, приведены в ГОСТ Р 58833 и ГОСТ Р 70262.1;

- аутентификацию, включающую проверку подлинности субъекта (объекта) доступа и принадлежности ему предъявленных идентификатора и аутентификатора;

Примечание – Состав и содержание процесса аутентификации, включая действия, выполняемые участниками процесса, приведены в ГОСТ Р «Защита информации. Идентификация и аутентификация. Уровни доверия аутентификации» (проект);

- управление идентификацией и аутентификацей, включая организацию и поддержание деятельности участников процессов идентификации и аутентификации, в соответствии с правилами (политиками), принятыми в рамках структуры управления идентификацией и аутентификацией, а также управление выпуском, регистрацией, хранением и поддержанием актуального состояния (обновление), предоставлением для использования электронных удостоверений, прекращением их действия и отзывом.

Примечание – Состав и содержание процесса аутентификации, включая действия, выполняемые участниками процесса, приведены в проекте национального стандарта ГОСТ Р «Защита информации. Идентификация и аутентификация. Управление идентификацией и аутентификацией» (проект).

ГОСТ Р
(проект, первая редакция)

4.2 В соответствии с ГОСТ Р «Защита информации. Идентификация и аутентификация. Управление идентификацией и аутентификацией» (проект) в управлении идентификацией и аутентификацией в рамках структуры управления идентификацией и аутентификацией участвуют:

Примечание – Общая характеристика сторон, участвующих в управлении идентификацией и аутентификацией, в том числе взаимодействующих сторон, приведена в ГОСТ ISO/IEC 24760-2;

- орган регулирования. Сущность, осуществляющая надзор за соответствием политик и процедур, а также за соответствием их выполнения правовым и нормативным требованиям, а также за выполнением требований по защите информации;

- представитель физического лица. Сущность, осуществляющая контроль за соблюдением прав субъектов – физических лиц при обработке идентификационных данных;

Примечание – Представитель физического лица, который может представлять собой общественную организацию или группу лиц;

- взаимодействующие (действующие) стороны (сущности). Стороны (сущности), которые непосредственно участвуют в обмене идентификационными данными, и при необходимости аутентификационной информацией.

4.3 В соответствии с ГОСТ ISO/IEC 24760-2 и ГОСТ Р «Защита информации. Идентификация и аутентификация. Управление идентификацией и аутентификацией» (проект) в рамках структуры управления идентификацией и аутентификацией взаимодействующими (действующими) сущностями (сторонами), которые непосредственно обмениваются идентификационными данными и электронными удостоверениями, являются:

- субъект (объект) доступа. Действующая сущность, которая в рамках управления идентификацией и аутентификацией предоставляет (заявляет) идентификационные данные для установления и подтверждения

ее подлинности, а также предоставляет электронное удостоверение (идентификатор доступа и аутентификатор) для получения доступа;

- поставщик идентификационной информации. Действующая сущность, которая получает от сущности, заявившей запрос на регистрацию (субъекта или объекта доступа), осуществляет их верификацию и представляет идентификационные данные конкретной сущности (конкретного заявителя) для регистрации;

- орган регистрации. Действующая сущность, которая осуществляет регистрацию и поддержание актуальности идентификационной и аутентификационной информации;

- орган идентификационной информации. Действующая сущность, которая предоставляет электронные удостоверения сущностей, известных в домене;

- получатель электронного удостоверения[1]. Действующая сущность, которая полагается на идентификационную и аутентификационную информацию электронного удостоверения, предоставленного органом идентификационной информации, и применяет их в своей деятельности;

- орган проверки идентификационной информации[2]. Действующая сущность, отвечающая за установление достоверности и подлинности идентификационной информации, относящейся к конкретной сущности;

- орган управления идентичностью. Действующая сущность, отвечающая за создание и обеспечение соблюдения правил (политик), принятых участниками структуры управления идентификацией и аутентифи-

[1] По ГОСТ ISO/IEC 24760-2 – полагающая сторона. Термин уточнен для настоящего документа с целью отличия от понятий, определенных в ГОСТ Р 58833.

[2] По ГОСТ ISO/IEC 24760-2 – проверяющая сторона. Термин уточнен для настоящего документа с целью отличия от понятий, определенных в ГОСТ Р 58833.

кацией;

- орган контроля и аудита (аудитор). Действующая сущность, которая контролирует и подтверждает соответствие функционирования структуры управления идентификацией и аутентификацией документально оформленным политикам и процедурам, а также иным внешним требованиям органов регулирования (при необходимости).

Для реализации процессов управления идентификацией и аутентификацией между взаимодействующими (действующими) сущностями (сторонами) структуры управления идентификацией и аутентификацией следует использовать систему управления идентификацией и аутентификацией.

5 Рекомендации по управлению идентификацией и аутентификацией

5.1 В рамках структуры управления идентификацией и аутентификацией с учетом положений ГОСТ ISO/IEC 24760-2 и ГОСТ Р «Защита информации. Идентификация и аутентификация. Управление идентификацией и аутентификацией» (проект) должны быть реализованы:

- процесс надзора (контроля) за соответствием политик и процедур, определяющих функционирование структуры управления идентификацией и аутентификацией, а также за соответствием их выполнением требований, установленных соответствующими нормативными правовыми актами и методическими документами;

- процесс контроля за соблюдением прав субъектов – физических лиц при обработке идентификационных данных;

- процессы системы управления идентификацией и аутентификацией.

5.2 В рамках процесса надзора (контроля) за соответствием политик и процедур орган регулирования должен контролировать, что политики и процедуры соответствуют требованиям нормативных правовых актов и нормативных документов. При этом действующим сторонам необходимо выполнять следующие рекомендации:

- политики и процедуры, определяющие функционирование структуры управления идентификацией и аутентификацией, не должны противоречить требованиям соответствующих нормативных правовых актов, методических документов и документов по стандартизации;

- политики и процедуры, определяющие функционирование структуры управления идентификацией и аутентификацией следует документально оформлять, утверждать и вводить в действие установленным порядком;

- применение политик и процедур, включая реализацию необходимых мер защиты, необходимо периодически контролировать с подготовкой отчетов и представлением результатов в органы регулирования.

Примечание – Необходимость и периодичность представления результатов применения политик и процедур в органы регулирования определяется соответствующими нормативными правовыми актами.

5.3 В рамках процесса контроля за соблюдением прав субъектов – физических лиц при обработке идентификационных данных представитель физического лица должен осуществлять контроль выполнения требований соответствующих нормативных правовых актов.

Примечание – Представитель физического лица, может контролировать, например, соблюдение прав при обработке персональных данных в соответствии с требованиями [7].

При этом действующим сторонам необходимо следовать следующим рекомендациям:

- разработать и реализовать политики обработки персональных данных, включая регламентацию сбора, обработки, хранения, управле-

ния доступом, предоставления для использования;

- реализовать механизмы, включая методы, средства и технологии, обеспечивающие минимальное раскрытие персональных данных при обработке идентификационных данных в системе управления идентификацией и аутентификацией;

- обеспечить управление доступом и проверку подлинности сущностей, использующих идентификационную информацию, содержащую персональные данные;

- минимизировать возможность связывания идентичностей, принадлежащих разным доменам;

- обеспечить проведение аудита использования идентификационной информации;

- обеспечить защиту от возможного нарушения конфиденциальности персональных данных.

5.4 В рамках системы управления идентификацией и аутентификацией с учетом положений ГОСТ Р 58833, ГОСТ Р 59515, ГОСТ Р 70262.1, ГОСТ ISO/IEC 24760-2 и ГОСТ Р «Защита информации. Идентификация и аутентификация. Управление идентификацией и аутентификацией» (проект) должны быть реализованы:

- процесс представления идентификационных данных сущностью;

- процесс обработки и предоставления идентификационной и аутентификационной информации взаимодействующим сторонам, включая реализацию мер защиты используемой информации (см. раздел 6).

5.5 В рамках процесса представления идентификационных данных сущностью взаимодействующие (действующие) сущности должны провести первичную идентификацию заявителя, включая, распознавание, подготовку, верификацию, формирование и регистрацию идентификационной и аутентификационной информации сущности, а также присвоение и регистрацию идентификатора доступа субъекта (объекта) доступа

в перечне(-ях) идентификаторов доступа. При этом действующим сторонам необходимо следовать следующим рекомендациям:

- требования к первичной идентификации необходимо включать в политики и процедуры, определяющие сбор идентификационных данных, и документально оформлять, утверждать и вводить в действие установленным порядком;

- поставщику идентификационной информации следует запрашивать минимально необходимый объем идентификационных данных, достаточный для однозначной идентификации сущности в домене с необходимой уверенностью;

- сущности, заявившей запрос на регистрацию, необходимо предоставлять для внесения в реестр идентичностей идентификационные данные, соответствующие требованиям к первичной идентификации, подтвержденные свидетельствами идентичности;

- поставщику идентификационной информации для заявленных идентификационных данных следует (если определено политиками) выполнить проверку их существования путем их верификации и получения свидетельств от органа проверки идентификационной информации, и выполнить привязку верифицированных идентификационных данных к сущности;

- органу регистрации надлежит регистрировать идентификационную информацию и утверждать все ее изменения, а также определять, отслеживать и утверждать политики и процедуры формирования и изменения идентификационной информации, зафиксированной в реестре идентичностей;

- органу управления идентификационной информацией следует определить и контролировать выполнение взаимодействующими сущностями согласованных мер защиты информации (см. раздел 6).

ГОСТ Р
(проект, первая редакция)

5.6 В рамках процесса обработки идентификационной и аутентификационной информации взаимодействующие (действующие) сущности должны обеспечить обработку, поддержание актуальности и предоставление правильной и достоверной идентификационной и аутентификационной информации, включая реализацию мер защиты используемой информации. При этом необходимо руководствоваться следующим рекомендациям:

- все взаимодействующие (действующие) сущности обработку идентификационной и аутентификационной информации должны осуществлять в соответствии с правилами, регламентируемыми политиками и процедурами, которые следует документально оформлять, утверждать и вводить в действие установленным порядком;

- состав операций доступа к идентификационной и аутентификационной информации для субъекта (объекта) доступа и получателя электронного удостоверения необходимо определять до начала ее обработки;

- органу регистрации необходимо поддерживать актуальность идентификационной и аутентификационной информации;

- органу идентификационной информации передачу электронного удостоверения получателю следует выполнять по защищенным каналам передачи, либо способом, подтверждающим его получение подлинной сущностью. Активацию органом идентификационной информации электронного удостоверения следует выполнять непосредственно после получения получателем электронного удостоверения;

- органу управления идентичностью следует определить и контролировать выполнение взаимодействующими сущностями согласованных мер защиты информации (см. раздел 6) при ее обработке и хранении, а также при обмене ею между участвующими сущностями;

- получателю электронного удостоверения следует использовать только проверенную информацию, правильность и достоверность которой подтверждена органом идентификационной информации, для предоставления доступа к находящимся под его контролем услугам и ресурсам;

- взаимодействующим сущностям (сторонам) надлежит определить действия, подлежащие регистрации, и несоответствия, о которых следует сообщать органу управления идентичностью, а также установить необходимую детализацию состава и содержания регистрационной информации;

- органу контроля и аудита (аудитору) необходимо выполнять периодический контроль соответствия обработки идентификационной и аутентификационной информации требованиям политик и процедур, при этом органу управления идентичностью надлежит корректировать политики и процедуры с целью реализации любых рекомендованных изменений.

6 Рекомендации по мерам защиты от угроз процессам идентификации и аутентификации

6.1 Участники процессов идентификации и аутентификации должны обеспечивать защиту идентификационной и аутентификационной информации. При этом должно обеспечиваться исключение (уменьшение) возможности воздействия на нее вследствие реализации угроз,

в том числе осуществляемой и посредством эксплуатации нарушителем уязвимостей процессов идентификации и аутентификации [1].

6.2 Состав мер защиты от угроз процессам идентификации и аутентификации в конкретной среде функционирования следует формировать на основе перечня мер защиты, применяемых для исключения (уменьшения) возможности реализации типовых угроз процессам идентификации и аутентификации (см. Приложение А) в зависимости от их актуальности. Актуальность мер защиты и необходимость их применения определяется исходя из угроз процессам идентификации и аутентификации, актуальных для конкретной среды функционирования.

6.3 Описание мер защиты включает:

- идентификатор угрозы. Идентификатор угрозы однозначно идентифицирует угрозу в рамках перечня типовых угроз процессам идентификации и аутентификации;

Примечание – Дополнительно идентификатор угрозы связывает угрозу с ее описанием, приведенным в ГОСТ Р «Защита информации. Идентификация и аутентификация. Типовые угрозы и уязвимости процессов идентификации и аутентификации» (проект), а также с идентификатором и соответствующим описанием мер защиты;

- наименование угрозы. Условное наименование отражает в общем виде целевую направленность угрозы;

- описание угрозы. Описание определяет и конкретизирует основное содержание угрозы;

- идентификатор мер защиты. Идентификатор мер защиты однозначно идентифицирует совокупность мер защиты, которые применяют-

[1] Перечень типовых угроз и уязвимостей процессов идентификации и аутентификации приведен в ГОСТ Р «Защита информации. Идентификация и аутентификация. Типовые угрозы и уязвимости процессов идентификации и аутентификации» (проект).

ся для исключения (уменьшения) возможности реализации типовых угроз процессам идентификации и аутентификации, в рамках перечня мер защиты;

- меры защиты, применяемые для исключения (уменьшения) возможности реализации угрозы. Перечень устанавливает общий состав и содержание мер защиты, которые применяются для исключения (уменьшения) возможности реализации типовой угрозы процессам идентификации и аутентификации;

- реализация мер защиты в средствах и системах. Перечень определяет общее описание возможных методов и средств, которые могут быть использованы для реализации предлагаемых мер защиты.

6.4 Приведенные в настоящем документе меры защиты, не определяют их конкретную программную или программно-аппаратную (программно-техническую) реализацию в средствах защиты информации, средствах обеспечения безопасности информационных технологий, средствах вычислительной техники и автоматизированных, информационных и других системах. Конкретные программные или программно-аппаратные (программно-технические) реализации мер защиты в средствах и системах формируются с учетом рекомендаций, приведенных в приложении А, на основании требований, устанавливаемых соответствующими нормативными правовыми актами и методическими документами федеральных органов исполнительной власти, например [9], [10], и/или документами по стандартизации, например [11].

Приложение А
(обязательное)
Перечень мер защиты, применяемых для исключения (уменьшения) потенциально возможного воздействия типовых угроз процессам идентификации и аутентификации

Перечень и общая характеристика мер защиты, применяемых для исключения (уменьшения) потенциально возможного воздействия типовых угроз процессу первичной идентификации приведены в Таблице А.1. Перечень и общая характеристика мер защиты, применяемых для исключения (уменьшения) потенциально возможного воздействия типовых угроз процессам вторичной идентификации и аутентификации приведены в Таблице А.2. Перечень и общая характеристика мер защиты, применяемых для исключения (уменьшения) потенциально возможного воздействия типовых угроз процессам управления идентификацией и аутентификацией приведены в Таблице А.3.

Примечание – Общая характеристика угроз – по ГОСТ Р «Защита информации. Идентификация и аутентификация. Типовые угрозы и уязвимости процессов идентификации и аутентификации» (проект).

Таблица А.1 – Перечень мер защиты, применяемых для исключения (уменьшения) возможности реализации типовых угроз процессу первичной идентификации

Идентификатор угрозы	Наименование угрозы	Описание угрозы	Идентификатор мер защиты	Меры защиты, применяемые для исключения (уменьшения) возможности реализации угроз	Реализация мер защиты в средствах и системах
ПИ-1	Подмена свидетельства идентичности	Незаконное (мошенническое) использование идентификационных данных	ЗПИ-1	Использование политики подтверждения идентификационных данных[1] при первичной идентификации. Сущность должна предоставить идентификационные данные, как минимум, из одного источника, соответствующего политике. Представленные идентификационные данные должны подвергаться верификации	Разработка и публикация политики подтверждения идентификационных данных, и выполнение действий в процессе подтверждения в соответствии с опубликованной политикой. Необходимо проверить уникальность, существование заявленных идентификационных данных путем верификации и выполнить их привязку (установить или проверить связь) к сущности[2]
ПИ-2	Фальсификация свидетельств идентичности	Фальсификация свидетельств идентичности и/или их носителей	ЗПИ-2	Проверка носителей и свидетельств идентичности на соответствие установленным требованиям. Проверка свидетельств идентичности с помощью верифицирующей стороны	Проверка свидетельства идентичности должна включать: – проверку информации в свидетельстве идентичности в отношении упущений, ошибок и противоречий в идентификационных данных; – проверку каждого элемента носителя свидетельства идентичности на предмет его физической структуры, качества материала, качества печати, функций защиты, печатей и подписей.

[1] Политика подтверждения идентификационных данных, как правило, является составной частью политики информационной безопасности (организации).

[2] Более подробно см. ГОСТ Р 70262.1 и ГОСТ Р 59515.

Продолжение таблицы А.1

Идентификатор угрозы	Наименование угрозы	Описание угрозы	Идентификатор мер защиты	Меры защиты, применяемые для исключения (уменьшения) возможности реализации угроз	Реализация мер защиты в средствах и системах
					Проверки должны осуществлять квалифицированные специалисты, обладающие навыками, инструментальными средствами и способностями обнаружения поддельных или фальсифицированных носителей свидетельств идентичности [1]
ПИ-3	Подмена участвующей стороны	Подмена стороны, участвующей в первичной идентификации	ЗПИ-3	Проверка должна осуществляться в личном присутствии физического лица. Проверка должна осуществляться с применением, по возможности, фото и видеосъемки	Проверка должна осуществляться в личном присутствии физического лица, при этом: – лицо должно обладать свидетельством идентичности (документом); – свидетельство идентичности (документ) должно быть подлинным; – свидетельство идентичности (документ) должен быть проверен по источникам, которые предоставляются верифицирующей стороной (при необходимости уполномоченной верифицирующей стороной[2]); – необходимо выполнить привязку идентификационных данных (установить или проверить связь) с физическим лицом.

[1] Более подробно см. ГОСТ 59515.

[2] Более подробно см. ГОСТ Р 70262.1

Окончание таблицы А.1

Идентификатор угрозы	Наименование угрозы	Описание угрозы	Идентификатор мер защиты	Меры защиты, применяемые для исключения (уменьшения) возможности реализации угроз	Реализация мер защиты в средствах и системах
					Возможно удаленное проведение проверки (без личного присутствия) физического лица, при этом: – лицо должно предоставить подтверждение, что обладает идентификационными данными; – идентификационные данные должны быть проверены по источникам, которые предоставляются верифицирующей стороной (при необходимости уполномоченной верифицирующей стороной); – необходимо проверить информацию на ее соответствие ранее предоставленной (рекомендуется – предоставленной при личном присутствии); должны применяться методы обнаружения жизненности сущностей – физических лиц[1]
ПИ-4	Перехват при обмене	Перехват при обмене свидетельствами идентичности или идентификационными данными	ЗПИ-4	Передача свидетельств идентичности (подтверждающей информации) должна осуществляться безопасным способом	Передача свидетельств идентичности (подтверждающей информации) по защищенным каналам передачи данных. При этом необходимо учитывать возможность внесения изменений во время передачи, а также возможность отказа от факта предоставления подтверждающей информации

[1] Более подробно см. ГОСТ Р 59515.

Таблица А.2 – Перечень мер защиты, применяемых для исключения (уменьшения) возможности реализации типовых угроз процессам вторичной идентификации и аутентификации

Идентификатор угрозы	Наименование угрозы	Описание угрозы	Идентификатор мер защиты	Меры защиты, применяемые для исключения (уменьшения) возможности реализации угроз	Реализация мер защиты в средствах и системах
ИА-1	Фишинг	Подмена участвующей стороны	ЗИА-1	Использование взаимной аутентификации доказывающей стороны и доверяющей стороны (проверяющей стороны – при ее наличии) с использованием криптографических алгоритмов	Строгая аутентификация средств вычислительной техники
				Использование политики использования информационных ресурсов	Разработка и публикация политики использования информационных ресурсов пользователями, включающей, в том числе способы противодействия методам социальной инженерии, и выполнение действий в процессе взаимодействия сторон в соответствии с опубликованной политикой
ИА-2	Фарминг	Перенаправление участвующей стороны	ЗИА-2	Использование взаимной аутентификации доказывающей стороны и доверяющей стороны (проверяющей стороны – при ее наличии) с использованием криптографических алгоритмов	Строгая аутентификация средств вычислительной техники

Продолжение таблицы А.2

Идентификатор угрозы	Наименование угрозы	Описание угрозы	Идентификатор мер защиты	Меры защиты, применяемые для исключения (уменьшения) возможности реализации угроз	Реализация мер защиты в средствах и системах
ИА-3	Прослушивание	Пассивное прослушивание нарушителем сеанса аутентификации	ЗИА-3	Должны использоваться механизмы аутентификации, не передающие секреты по каналам обмена или использующие обмен с применением криптографических алгоритмов. Для каждого сеанса аутентификации следует использовать разные идентификаторы сеанса и параметры аутентификации. Необходимо, чтобы секреты привязки сеанса генерировались доказывающей стороной во время взаимодействия после аутентификации и имели конечный срок действия	Усиленная аутентификация пользователей средств вычислительной техники с использованием следующих средств аутентификации[1]: многофакторный генератор одноразовых паролей или совместно с запоминаемым секретом должны использоваться поисковый секрет или внеполосное устройство или однофакторный генератор одноразовых паролей или однофакторное криптографическое программное средство аутентификации или однофакторное криптографическое техническое средство аутентификации. Строгая аутентификация пользователей средств вычислительной техники с использованием следующих средств аутентификации: – многофакторное криптографическое техническое средство аутентификации или

[1] Характеристика аутентификаторов приведена в ГОСТ Р «Защита информации. Идентификация и аутентификация. Уровни доверия аутентификации» (проект).

Продолжение таблицы А.2

Идентификатор угрозы	Наименование угрозы	Описание угрозы	Идентификатор мер защиты	Меры защиты, применяемые для исключения (уменьшения) возможности реализации угроз	Реализация мер защиты в средствах и системах
					– однофакторное криптографическое техническое средство аутентификации совместно с запоминаемым секретом или многофакторный генератор одноразовых паролей (техническое устройство или программный генератор) совместно с однофакторным криптографическим техническим средством аутентификации или однофакторный технический генератор одноразовых паролей совместно с многофакторным криптографическим программным средством аутентификации. Строгая аутентификация средств вычислительной техники
ИА-4	Повторное воспроизведение	Повторное воспроизведение сеанса аутентификации	ЗИА-4	Для каждого сеанса аутентификации следует использовать разные идентификаторы сеанса и параметры аутентификации. На каждом сообщении сеанса аутентификации должна быть проставлена не поддающаяся подделке отметка времени	Строгая аутентификация средств вычислительной техники
ИА-5	Перехват сеанса	Перехват обмена аутентификационными сообщениями	ЗИА-5	Должно использоваться взаимное подтверждение установления связи с использованием криптографических алгоритмов	Строгая аутентификация средств вычислительной техники

Продолжение таблицы А.2

Идентификатор угрозы	Наименование угрозы	Описание угрозы	Идентификатор мер защиты	Меры защиты, применяемые для исключения (уменьшения) возможности реализации угроз	Реализация мер защиты в средствах и системах
ИА-6	«Человек посередине»	Организация поддельного обмена данными между участвующими сторонами	ЗИА-6	Должна использоваться взаимная аутентификация доказывающей стороны и проверяющей (доверяющей) стороны с использованием криптографических алгоритмов	Строгая аутентификация средств вычислительной техники
ИА-7	Спуфинг	Выдача себя за другого	ЗИА-7	Необходимо использовать электронные удостоверения, которые должны верифицироваться с использованием третьей стороны	Строгая аутентификация средств вычислительной техники с использованием третьей стороны. Строгая аутентификация пользователей средств вычислительной техники с использованием третьей стороны и применением следующих средств аутентификации: – многофакторное криптографическое техническое средство аутентификации или – однофакторное криптографическое техническое средство аутентификации совместно с запоминаемым секретом или многофакторный генератор одноразовых паролей (техническое устройство или программный генератор) совместно с однофакторным криптографическим

Продолжение таблицы А.2

Идентификатор угрозы	Наименование угрозы	Описание угрозы	Идентификатор мер защиты	Меры защиты, применяемые для исключения (уменьшения) возможности реализации угроз	Реализация мер защиты в средствах и системах
					техническим средством аутентификации или однофакторный технический генератор одноразовых паролей совместно с многофакторным криптографическим программным средством аутентификации
ИА-8, ИА-9	Хищение или утеря аутентификатора	Аутентификатор может быть похищен или утерян владельцем	ЗИА-8.9	Использование многофакторных аутентификаторов, которые необходимо активировать, используя запоминаемый секрет или биометрические данные	Строгая аутентификация пользователей средств вычислительной техники с использованием следующих средств аутентификации: многофакторный генератор одноразовых паролей, многофакторное криптографическое программное средство, многофакторное криптографическое техническое средство аутентификации, многофакторное криптографическое техническое средство аутентификации с неизвлекаемым ключом. Использование устройств аутентификации с защитой от вмешательства, которые обнуляются после определенного числа неуспешных попыток использования

Продолжение таблицы А.2

Идентификатор угрозы	Наименование угрозы	Описание угрозы	Идентификатор мер защиты	Меры защиты, применяемые для исключения (уменьшения) возможности реализации угроз	Реализация мер защиты в средствах и системах
				Использование комбинации аутентификаторов, включающей однофакторный аутентификатор и запоминаемый секрет или биометрические данные	Усиленная или строгая аутентификация пользователей средств вычислительной техники с помощью следующих средств аутентификации: совместно с запоминаемым секретом должны использоваться поисковый секрет или внеполосное устройство или однофакторный генератор одноразовых паролей или однофакторное криптографическое программное средство аутентификации или однофакторное криптографическое техническое средство аутентификации. Использование устройств аутентификации с защитой от вмешательства, которые обнуляются после определенного числа неуспешных попыток использования
				Использование политики применения и хранения аутентификаторов	Формирование и ведение списка известных скомпрометированных аутентификаторов. Обучение физических лиц правильному хранению аутентификаторов действиям при их компрометации

Продолжение таблицы А.2

Идентификатор угрозы	Наименование угрозы	Описание угрозы	Идентификатор мер защиты	Меры защиты, применяемые для исключения (уменьшения) возможности реализации угроз	Реализация мер защиты в средствах и системах
ИА-10	Обнаружение данных	Раскрытие данных, необходимых для аутентификации	ЗИА-10	Использование политики применения и хранения аутентификаторов	Предотвращение раскрытия персональной (индивидуальной) информации, которая не может быть открытой и которая используется для ответа на запрос проверяющей (доверяющей) стороны
ИА-11	Дублирование аутентификатора	Незаконное копирование аутентификатора и последующее использование копии	ЗИА-11	Передача аутентификаторов по каналу, защищенному с использованием криптографических алгоритмов. Использование электронных удостоверений с динамически изменяющимися секретами	Использование методов (протоколов) устойчивых к повторному воспроизведению (см. угрозу ИА-4): использование строгой аутентификации средств вычислительной техники
ИА-12	Отгадывание в реальном времени	Отгадывание секрета в реальном времени (во время аутентификации)	ЗИА-12	Реализация правил, которые препятствуют выбору распространенных легко отгадываемых секретов, а также правил, которые обеспечивают генерацию секретов, имеющих высокую энтропию. Мониторинг попыток аутентификации и ограничение числа разрешенных неуспешных попыток аутентификации, а также частоты попыток аутентификации	Простая аутентификация пользователей средств вычислительной техники с помощью следующих средств аутентификации: запоминаемый секрет, поисковый секрет, однофакторный генератор одноразовых паролей. Аутентификаторы формируются с применением правил, которые препятствуют выбору распространенных легко отгадываемых секретов, либо обеспечивают генерацию секретов, имеющих высокую энтропию

Продолжение таблицы А.2

Идентификатор угрозы	Наименование угрозы	Описание угрозы	Идентификатор мер защиты	Меры защиты, применяемые для исключения (уменьшения) возможности реализации угроз	Реализация мер защиты в средствах и системах
				Использование политики формирования и хранения запоминаемых секретов	Разработка и публикация политики формирования и хранения запоминаемых секретов, и выполнение действий в процессе подтверждения в соответствии с опубликованной политикой
ИА-13	Отгадывание вне сеанса	Отгадывание секрета вне сеанса аутентификации (не во время аутентификации)	ЗИА-13	Использование устройств аутентификации с наличием блокировки после ряда повторяющихся неуспешных попыток активации и/или использующих для активации секреты, имеющие высокую энтропию	Строгая аутентификация пользователей средств вычислительной техники с помощью следующих средств аутентификации: многофакторный генератор одноразовых паролей, многофакторное криптографическое программное средство аутентификации, многофакторное криптографическое техническое средство аутентификации, многофакторное криптографическое техническое средство аутентификации с неизвлекаемым ключом
				Использование политики формирования и хранения секретов для активации устройств аутентификации	Разработка и публикация политики формирования и хранения секретов для активации устройств аутентификации, и выполнение действий в процессе подтверждения в соответствии с опубликованной политикой

Продолжение таблицы А.2

Идентификатор угрозы	Наименование угрозы	Описание угрозы	Идентификатор мер защиты	Меры защиты, применяемые для исключения (уменьшения) возможности реализации угроз	Реализация мер защиты в средствах и системах
ИА-14	Создание/модификация аутентификационного утверждения	Подмена данных в аутентификационном утверждении для того, чтобы выдать нарушителя за легальную сущность	ЗИА-14	Использование взаимно аутентифицированного сеанса между сторонами и протокола аутентификации, защищенного с использованием криптографических алгоритмов. Стороны должны быть аутентифицированы до начала обмена. Допускается использование любого протокола, требующего, чтобы серия сообщений между двумя сторонами была подписана их источником и зашифрована для получателя. Допускается подписание утверждения электронной подписью проверяющей стороны	Строгая аутентификация средств вычислительной техники. Строгая аутентификация пользователей средств вычислительной техники с помощью следующих средств аутентификации: – многофакторное криптографическое техническое средство аутентификации или – однофакторное криптографическое техническое средство аутентификации совместно с запоминаемым секретом или многофакторный генератор одноразовых паролей (техническое устройство или программный генератор) совместно с однофакторным криптографическим техническим средством аутентификации или однофакторный технический генератор одноразовых паролей совместно с многофакторным криптографическим программным средством аутентификации

Продолжение таблицы А.2

Идентификатор угрозы	Наименование угрозы	Описание угрозы	Идентификатор мер защиты	Меры защиты, применяемые для исключения (уменьшения) возможности реализации угроз	Реализация мер защиты в средствах и системах
ИА-15	Раскрытие аутентификационного утверждения	Перехват и ознакомление с содержанием информации аутентификационного утверждения для ее несанкционированного использования	ЗИА-15	Использование взаимно аутентифицированного сеанса между сторонами и протокола аутентификации, защищенного с использованием криптографических алгоритмов. Стороны должны быть аутентифицированы до начала обмена. Допускается использование любого протокола, требующего, чтобы серия сообщений между двумя сторонами была подписана их источником и зашифрована для получателя. Допускается подписание утверждения электронной подписью проверяющей стороны	Строгая аутентификация средств вычислительной техники. Строгая аутентификация пользователей средств вычислительной техники с помощью следующих средств аутентификации: – многофакторное криптографическое техническое средство аутентификации или – однофакторное криптографическое техническое средство аутентификации совместно с запоминаемым секретом или многофакторный генератор одноразовых паролей (техническое устройство или программный генератор) совместно однофакторным криптографическим техническим средством аутентификации или однофакторный технический генератор одноразовых паролей совместно с многофакторным криптографическим программным средством аутентификации

Продолжение таблицы А.2

Идентификатор угрозы	Наименование угрозы	Описание угрозы	Идентификатор мер защиты	Меры защиты, применяемые для исключения (уменьшения) возможности реализации угроз	Реализация мер защиты в средствах и системах
ИА-16	Отрицание аутентификационного утверждения проверяющей стороной	Выдача аутентификационного утверждения отрицается проверяющей стороной	ЗИА-16	Выдача аутентификационного утверждения, снабженного электронной подписью проверяющей стороны, поддерживающей неотказуемость	Строгая аутентификация средств вычислительной техники. Строгая аутентификация пользователей средств вычислительной техники с помощью следующих средств аутентификации: многофакторное криптографическое программное средство аутентификации, многофакторное криптографическое техническое средство аутентификации, многофакторное криптографическое техническое средство аутентификации с неизвлекаемым ключом
ИА-17	Отрицание аутентификационного утверждения доказывающей стороной	Передача аутентификационного утверждения отрицается доказывающей стороной	ЗИА-17	Выдача проверяющей стороной аутентификационного утверждения на владельца[1] – доказывающую сторону	Строгая аутентификация средств вычислительной техники. Строгая аутентификация пользователей средств вычислительной техники с помощью следующих средств аутентификации: многофакторное криптографическое программное средство аутентификации, многофакторное криптографическое техническое средство

[1] Подробно об утверждении на владельца – ГОСТ Р Защита информации. Идентификация и аутентификация. Уровни доверия аутентификации (проект).

Продолжение таблицы А.2

Идентификатор угрозы	Наименование угрозы	Описание угрозы	Идентификатор мер защиты	Меры защиты, применяемые для исключения (уменьшения) возможности реализации угроз	Реализация мер защиты в средствах и системах
					аутентификации, многофакторное криптографическое техническое средство аутентификации с неизвлекаемым ключом
ИА-18	Перенаправление аутентификационного утверждения	Перенаправление аутентификационного утверждения, предназначенного одной доверяющей стороне другой доверяющей стороне	ЗИА-18	Аутентификационное утверждение должно включать идентификационные данные доверяющей стороны, для которой оно было сгенерировано	Строгая аутентификация средств вычислительной техники. Строгая аутентификация пользователей средств вычислительной техники с помощью следующих средств аутентификации: многофакторное криптографическое программное средство аутентификации, многофакторное криптографическое техническое средство аутентификации, многофакторное криптографическое техническое средство аутентификации с неизвлекаемым ключом
ИА-19	Повторное использование аутентификационного утверждения	Повторное использование аутентификационного утверждения, которое уже однажды использовалось	ЗИА-19	Выпуск аутентификационного утверждения с меткой времени на определенный, минимально возможный, срок действия. Значение срока действия может быть включено в аутентификационное утверждение или может устанавливаться доверяющей стороной	Строгая аутентификация средств вычислительной техники. Строгая аутентификация пользователей средств вычислительной техники с помощью следующих средств аутентификации: многофакторное криптографическое программное средство аутентификации, многофакторное криптографическое техническое средство аутентификации, многофакторное криптографическое техническое средство аутентификации с неизвлекаемым ключом

Продолжение таблицы А.2

Идентификатор угрозы	Наименование угрозы	Описание угрозы	Идентификатор мер защиты	Меры защиты, применяемые для исключения (уменьшения) возможности реализации угроз	Реализация мер защиты в средствах и системах
ИА-20	Создание вторичного аутентификатора	Создание вторичного аутентификатора[1] для аутентифицированной доказывающей стороны	ЗИА-20	Выпуск аутентификационного утверждения, имеющего высокую энтропию. Вторичный аутентификатор может содержать временные данные утверждения, подписанные проверяющей стороной. Допускается, чтобы доказывающая сторона аутентифицировалась непосредственно у доверяющей стороны, используя свой долгосрочный секрет	Строгая аутентификация средств вычислительной техники. Строгая аутентификация пользователей средств вычислительной техники с помощью следующих средств аутентификации: – многофакторное криптографическое техническое средство аутентификации или – однофакторное криптографическое техническое средство аутентификации совместно с запоминаемым секретом или многофакторный генератор одноразовых паролей (техническое устройство или программный генератор) совместно однофакторным криптографическим техническим средством аутентификации или однофакторный технический генератор одноразовых паролей совместно с многофакторным криптографическим программным средством аутентификации

[1] Подробно о вторичном аутентификаторе – ГОСТ Р Защита информации. Идентификация и аутентификация. Уровни доверия аутентификации (проект).

Идентификатор угрозы	Наименование угрозы	Описание угрозы	Идентификатор мер защиты	Меры защиты, применяемые для исключения (уменьшения) возможности реализации угроз	Реализация мер защиты в средствах и системах
ИА-21	Захват вторичного аутентификатора	Захват вторичного аутентификатора аутентифицированной доказывающей стороны	ЗИА-21	Необходимо, чтобы вторичный аутентификатор передавался через сеанс обмена сообщениями, установленный во время первичной аутентификации доказывающей стороны, защищенный с использованием криптографических алгоритмов, обеспечивающих защиту от подслушивания (ИА-4) и угрозы «человек посередине» (ИА-6). Вторичный аутентификатор не должен передаваться через незащищенный сеанс обмена сообщениями или не аутентифицированной стороне, пока он еще действителен. Если вторичный аутентификатор является характерным для единственной доверяющей стороны и если эта доверяющей сторона не будет принимать вторичные аутентификаторы с тем же значением, пока не истек срок действия соответствующего аутентификационного утверждения, то передача вторичного аутентификатора может осуществляться без защиты	Строгая аутентификация средств вычислительной техники. Строгая аутентификация пользователей средств вычислительной техники с помощью следующих средств аутентификации: – многофакторное криптографическое техническое средство аутентификации или – однофакторное криптографическое техническое средство аутентификации совместно с запоминаемым секретом или многофакторный генератор одноразовых паролей (техническое устройство или программный генератор) совместно однофакторным криптографическим техническим средством аутентификации или однофакторный технический генератор одноразовых паролей совместно с многофакторным криптографическим программным средством аутентификации

Окончание таблицы А.2

Идентификатор угрозы	Наименование угрозы	Описание угрозы	Идентификатор мер защиты	Меры защиты, применяемые для исключения (уменьшения) возможности реализации угроз	Реализация мер защиты в средствах и системах
ИА-22	Замена утверждения	Манипуляция данными аутентификационного утверждения, которые не связаны с вторичным аутентификатором аутентификационного утверждения	ЗИА-22	Ответы на запросы утверждений, подписанные проверяющей стороной, могут содержать значение ссылки на утверждение, использованное в запросе, или некоторый другой одноразовый код, который был привязан с использованием криптографических алгоритмов к запросу доверяющей стороной	Строгая аутентификация средств вычислительной техники. Строгая аутентификация пользователей средств вычислительной техники с помощью следующих средств аутентификации: многофакторное криптографическое программное средство аутентификации, многофакторное криптографическое техническое средство аутентификации, многофакторное криптографическое техническое средство аутентификации с неизвлекаемым ключом

Таблица А.3 – Перечень мер защиты, применяемых для исключения (уменьшения) возможности реализации типовых угроз процессам управления идентификацией и аутентификацией

Идентификатор угрозы	Наименование угрозы	Описание угрозы	Идентификатор мер защиты	Меры защиты, применяемые для исключения (уменьшения) возможности реализации угроз	Реализация мер защиты в средствах и системах
УИА-1	Подделка электронного удостоверения при выпуске	Информация, используемая для создания электронного удостоверения несанкционировано изменяется	ЗУИА-1	Для создания электронного удостоверения регистрирующая сторона должна использовать формализованные и документально оформленные процессы. До завершения привязки электронного удостоверения к сущности регистрирующая сторона должна быть уверена в том, что электронное удостоверение связано и остается связанным с надлежащей сущностью. Привязка электронного удостоверения должна обеспечивать защиту от подделки посредством использования электронной подписи или блокировкой электронного удостоверения, в том числе и содержащегося в устройстве аутентификации, до его активации	Разработка и публикация политики создания и применения электронного удостоверения, и выполнение действий в процессе создания электронного удостоверения в соответствии с опубликованной политикой. Использование при выпуске электронного удостоверения следующих средств аутентификации: однофакторный технический генератор одноразовых или многофакторный технический генератор одноразовых паролей или однофакторное криптографическое техническое средство аутентификации или многофакторное криптографическое техническое средство аутентификации или многофакторное криптографическое техническое средство аутентификации с неизвлекаемым ключом

Продолжение таблицы А.3

Идентификатор угрозы	Наименование угрозы	Описание угрозы	Идентификатор мер защиты	Меры защиты, применяемые для исключения (уменьшения) возможности реализации угроз	Реализация мер защиты в средствах и системах
УИА-2	Несанкционированный выпуск электронного удостоверения	Создание электронного удостоверения для несуществующей сущности	ЗУИА-2	Для создания электронного удостоверения регистрирующая сторона должна использовать формализованные и документально оформленные процессы	Разработка и публикация политики создания и применения электронного удостоверения, и выполнение действий в процессе создания электронного удостоверения в соответствии с опубликованной политикой. Для устройств аутентификации, которые используются для генерации и последующего хранения электронного удостоверения должна обеспечиваться физическая защита, учет и отслеживание его движения при создании
УИА-3	Хищение электронного удостоверения при выпуске	Выпущенное электронное удостоверение (или устройство аутентификации) копируется (клонируется) при транспортировке от отправителя (регистрирующей стороны) до получателя (сущности)	ЗУИА-3	Для выпуска электронного удостоверения регистрирующая сторона должна использовать формализованные и документально оформленные процессы. Процесс выпуска должен включать механизм, позволяющий удостовериться, что электронное удостоверение предоставляется подлинной сущности. Если оно не передается лично, должен существовать механизм для проверки существования адреса доставки и его легитимной связи с сущностью	Разработка и публикация политики создания и применения электронного удостоверения, и выполнение действий в процессе его создания и доставки сущности в соответствии с опубликованной политикой. Электронное удостоверение (и/или устройство аутентификации) должно доставляться безопасным образом (по защищенному каналу) и/или сущность должна подтвердить получение электронного удостоверения (и/или устройства аутентификации). Для подтверждения доставки и получения может использоваться внеполосное устройство

Продолжение таблицы А.3

Идентификатор угрозы	Наименование угрозы	Описание угрозы	Идентификатор мер защиты	Меры защиты, применяемые для исключения (уменьшения) возможности реализации угроз	Реализация мер защиты в средствах и системах
УИА-4	Активация незаконно полученного электронного удостоверения	Незаконно полученное электронное удостоверение активируется	ЗУИА-4	Регистрирующая сторона должна иметь политику (процедуру), позволяющую удостовериться, что электронное удостоверение активируются подлинной сущностью, для которой оно предназначено. При активации необходимо подтвердить, что сущность связана с активируемым электронным удостоверением (например, запросом и подтверждением). Необходимо, чтобы активация разрешалась только в течение временного периода, определенного политикой	Разработка и публикация политики создания и применения электронного удостоверения, и выполнение действий в процессе его создания и доставки сущности в соответствии с опубликованной политикой. Для активации электронного удостоверения может использоваться внеполосное устройство
УИА-5	Невозможность активации электронного удостоверения	Электронное удостоверение невозможно активировать ввиду отсутствия получателя (сущности) или невозможности доказать подлинность получателя (сущности) или ввиду нарушения сроков поставки	ЗУИА-5		

Продолжение таблицы А.3

Идентификатор угрозы	Наименование угрозы	Описание угрозы	Идентификатор мер защиты	Меры защиты, применяемые для исключения (уменьшения) возможности реализации угроз	Реализация мер защиты в средствах и системах
УИА-6	Хищение электронного удостоверения при хранении	Выпущенное электронное удостоверения (или устройство аутентификации) копируется (дублируется) при хранении	ЗУИА-6	Регистрирующая сторона должна установить политику защиты хранящихся электронных удостоверений, которая должна быть доступна для сущностей. От сущностей должно требоваться подтверждение (в том числе письменное) того, что они понимают эти требования и согласны обеспечивать защиту в соответствии с требованиями. Защита электронных удостоверений должна обеспечиваться с помощью управления доступом, в том числе с применением физической защиты устройств аутентификации. Хранилища не должны содержать электронные удостоверения в незашифрованном виде	Разработка и публикация политики создания и применения электронного удостоверения, и выполнение действий в процессе его создания и доставки сущности в соответствии с опубликованной политикой. Для защиты электронных удостоверений могут применяться средства управления доступом к информации и средства криптографической защиты информации. Для защиты устройств аутентификации могут использоваться средства физической защиты
УИА-7	Подделка электронного удостоверения при хранении	Подмена данных в электронном удостоверении при хранении	ЗУИА-7		
УИА-8	Раскрытие электронного удостоверения при хранении	Электронное удостоверение и/или устройство аутентификации становится общедоступным вследствие их хранения регистрирующей стороной или сущность ненадлежащим образом	ЗУИА-8		

Продолжение таблицы А.3

Идентификатор угрозы	Наименование угрозы	Описание угрозы	Идентификатор мер защиты	Меры защиты, применяемые для исключения (уменьшения) возможности реализации угроз	Реализация мер защиты в средствах и системах
УИА-9	Несвоевременное аннулирование электронного удостоверения	Задержка аннулирования электронного удостоверения	ЗУИА-9	Регистрирующая сторона должна аннулировать или уничтожать (если это возможно) электронные удостоверения в течение конкретного временного периода, который определен в политике организации	Разработка и публикация политики аннулирования электронных удостоверений, и выполнение действий в соответствии с опубликованной политикой. Использование средств публикации списков (реестров, перечней) отозванных аннулированных электронных удостоверений на средствах вычислительной техники
УИА-10	Использование неаннулированного электронного удостоверения	Использование неаннулированного электронного удостоверения несуществующей сущности	ЗУИА-10		

Продолжение таблицы А.3

Идентификатор угрозы	Наименование угрозы	Описание угрозы	Идентификатор мер защиты	Меры защиты, применяемые для исключения (уменьшения) возможности реализации угроз	Реализация мер защиты в средствах и системах
УИА-11	Хищение электронного удостоверения при продлении	Выпущенное электронное удостоверение (или устройство аутентификации) копируется (клонируется) при продлении	ЗУИА-11	Регистрирующая сторона должна установить политики продления и замены электронного удостоверения. При необходимости осуществляется подтверждение идентификационных данных мерами, обеспечивающими противодействие угрозе УИА-1. Все взаимодействия между регистрирующей стороной и сущностью должны осуществляться по защищенному каналу обмена данными	Разработка и публикация политики продления и замены электронного удостоверения, и выполнение действий в соответствии с опубликованной политикой. Сущность должна доказать обладание электронным удостоверением с неистекшим сроком действия, прежде чем регистрирующая сторона разрешит продление и/или замену. После истечения срока действия текущего электронного удостоверения продление не должно осуществляться. Защита канала обмена данными реализуется средствами криптографической защиты информации
УИА-12	Подделка электронного удостоверения при продлении	Подмена запроса (данных в запросе) для создания электронного удостоверения при продлении	ЗУИА-12		
УИА-13	Несанкционированное продление электронного удостоверения при продлении	Подача запроса для создания электронного удостоверения	ЗУИА-13		

Окончание таблицы А.3

Идентификатор угрозы	Наименование угрозы	Описание угрозы	Идентификатор мер защиты	Меры защиты, применяемые для исключения (уменьшения) возможности реализации угроз	Реализация мер защиты в средствах и системах
УИА-14	Отрицание получения электронного удостоверения	Отрицание получения подлинного электронного удостоверения подлинной сущностью	ЗУИА-14	Регистрирующая сторона должна поддерживать записи регистрации, истории и состояния каждого электронного удостоверения (включая аннулирование). Длительность хранения записей должна определяться политикой регистрирующей стороны. Для обеспечения сохранности каждой записи должны быть разработаны формализованные и документально оформленные процедуры.	Разработка и публикация политики хранения электронных удостоверений, и выполнение действий в соответствии с опубликованной политикой. Использование средств управления доступом к информации и защищенных носителей информации для хранения записей регистрации, истории существования и состояния каждого электронного удостоверения

ГОСТ Р
(проект, первая редакция)

Библиография

[1] NIST SP 800-63-3 Digital Identity Guidelines (Руководства по цифровым идентичностям)

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

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

[4] ITSP.30.031 User authentication guidance for information technology systems (Руководство по аутентификации пользователей для систем информационных технологий)

[5] ITU-T X.1254 (09/2020) Cyberspace security – Identity management – Entity authentication assurance framework (Безопасность киберпространства. Управление идентичностью. Структура доверия аутентификации сущности)

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

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

[8] Р 50.1.056–2005 Техническая защиты информации. Основные термины и определения

[9] Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» (Утверждены Приказом ФСТЭК России от 11 февраля 2013 года № 17)

[10] Требования к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды (Утверждены Приказом ФСТЭК России от 14 марта 2014 года № 31)

[11] ГОСТ 51624-2000 Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования

ГОСТ Р
(проект, первая редакция)

УДК 004:006.354 ОКС 35.030

Ключевые слова: защита информации, управление доступом, первичная идентификация, вторичная идентификация, аутентификация, идентификационная информация, аутентификационная информация, управление идентификацией и аутентификацией, меры защиты

Пояснительная записка

на первую редакцию проекта национального стандарта
ГОСТ Р «Защита информации. Идентификация и аутентификация.
Рекомендации по управлению идентификацией и аутентификацией»

1 Основание для разработки стандарта

Настоящий проект национального стандарта ГОСТ Р «Защита информации. Идентификация и аутентификация. Рекомендации по управлению идентификацией и аутентификацией» разрабатывается в соответствии с темой 1.11.362-1.026.23 Программы национальной стандартизации и Планом работы технического комитета по стандартизации ТК 362 «Защита информации» на 2024 год.

2 Краткая характеристика объекта и аспекта стандартизации

Объектом стандартизации разрабатываемого проекта национального стандарта являются процессы идентификации и аутентификации субъектов (объектов) доступа, а аспектом стандартизации – способы и правила управление идентификацией и аутентификацией субъектов и объектов доступа.

Целями стандартизации является создание условий:

- для защиты информации ограниченного доступа;
- для повышения уровня безопасности жизни и здоровья граждан, имущества физических и юридических лиц, государственного и муниципального имущества (за счет обеспечения безопасности обрабатываемой информации);
- для обеспечения конкурентоспособности, качества продукции и подтверждения соответствия продукции.

Проект национального стандарта ГОСТ Р «Защита информации. Идентификация и аутентификация. Рекомендации по управлению идентификацией и аутентификацией» включает следующие разделы:

- область применения;
- нормативные ссылки;
- термины и определения;
- общие положения;
- рекомендации по управлению идентификацией и аутентификацией;
- рекомендации по мерам защиты от угроз процессам идентификации и аутентификации;

- приложение;
- библиография.

3 Обоснование целесообразности разработки стандарта на национальном уровне и ожидаемый эффект от его применения

Необходимость разработки проекта национального стандарта ГОСТ Р «Защита информации. Идентификация и аутентификация. Рекомендации по управлению идентификацией и аутентификацией» была вызвана следующим.

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 определенному физическому лицу и конкретному информационному 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, к которым осуществляется доступ. Данное соответствие, как правило, устанавливается при регистрации ресурса как объекта или субъекта доступа и физического лица как пользователя (субъекта доступа), проверяется при опознавании субъекта доступа по предъявленному идентификатору доступа, подтверждается при проверке его подлинности и обеспечивает определенную уверенность в том, что обработка данных вычислительными процессами действительно инициирована физическим лицом или ресурсом, имеющим на это право. С целью поддержания актуальности, правильности, достоверности и регламентации использования информации (данных), которая применяется при принятии решений о возможности регистрации объекта (субъекта) доступа, соответствии между субъектом доступа и предъявленным идентификатором при идентификации и подлинности субъекта (объекта) при аутен-

тификации, необходимо управлять идентификацией и аутентификацией. Управление, осуществляется в рамках организационно-технической структуры, обеспечивающей формирование, администрирование и использование идентификационной и аутентификационной информации. При формировании данной структуры следует определить правила взаимодействия для сторон, участвующих в идентификации и аутентификации, а также реализовать защиту используемой информации (данных).

Проект национального стандарта определяет:

- базовый состав структуры управления идентификацией и аутентификацией, включая элементы структуры и возможные взаимодействие между ними;

- методы (способы) нейтрализации угроз и устранения уязвимостей, возникающих при идентификации и аутентификации, направленные на реализацию мер защиты информации в системе управления идентификацией и аутентификацией.

Принятие проекта национального стандарта ГОСТ Р «Защита информации. Идентификация и аутентификация. Рекомендации по управлению идентификацией и аутентификацией» позволит повысить эффективность мероприятий по обеспечению и поддержанию безопасности информации в организациях за счет превентивного определения стандартизированных мер защиты, устраняющих актуальные типовые угрозы и уязвимости процессов идентификации и аутентификации, при проектировании и создании автоматизированных (информационных) систем.

4 Сведения о соответствии проекта национального стандарта техническим регламентам Евразийского экономического союза, федеральным законам, техническим регламентам и иным нормативным правовым актам Российской Федерации

Проект национального стандарта разработан в соответствии с:

- Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

- Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»;

- ГОСТ Р 1.2–2020 Стандартизация в Российской Федерации. Стандарты национальные Российской Федерации. Правила разработки, утверждения, обновления, внесения поправок и отмены;

- ГОСТ Р 1.5–2012 Стандартизация в Российской Федерации. Стандарты национальные. Правила построения, изложения, оформления и обозначения.

5 Сведения о проведенных научно-исследовательских работах, технических предложениях, опытно-конструкторских, опытно-технологических и проектных работах, а также аналитических работах, послуживших основой для разработки проекта национального стандарта

При разработке проекта национального стандарта ГОСТ Р «Защита информации. Идентификация и аутентификация. Рекомендации по управлению идентификацией и аутентификацией» использовались результаты, полученные в рамках научно-исследовательской работы, выполняемой по заказу ФСТЭК России.

6 Сведения о соответствии проекта национального стандарта международному стандарту, региональному стандарту, региональному своду правил, стандарту иностранного государства и своду правил иностранного государства, иному документу по стандартизации иностранного государства

Проект национального стандарта не имеет в основе разработки международного стандарта, регионального стандарта, регионального свода правил, стандарта иностранного государства и свода правил иностранного государства.

7 Сведения о наличии в Федеральном информационном фонде стандартов переводов международных, региональных стандартов, стандартов и сводов правил иностранных государств, на которые даны нормативные ссылки в стандарте, использованном в качестве основы для разработки проекта национального стандарта Российской Федерации

Упомянутые переводы отсутствуют, т.к. в качестве основы международные, региональные стандарты и своды правил не использовались.

8 Сведения о взаимосвязи проекта национального стандарта с проектами или действующими в Российской Федерации другими национальными и межгосударственными стандартами, сводами правил, а при необходимости также предложения по их пересмотру, изменению или отмене

Проект национального стандарта ГОСТ Р «Защита информации. Идентификация и аутентификация. Рекомендации по управлению идентификацией и аутентификацией», определяя перечень типовых угроз безопасности и уязвимостей идентификации и аутентификации, позиционируется как составная часть следующего ком-

плекса стандартов, разрабатываемых в области идентификации и аутентификации, а также управления доступом:

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

- ГОСТ Р 59383-2021 Информационные технологии. Методы и средства обеспечения безопасности. Основы управления доступом;

- ГОСТ Р 70262.1-2022 Защита информации. Идентификация и аутентификация. Уровни доверия идентификации;

- ГОСТ Р Защита информации. Идентификация и аутентификация. Уровни доверия аутентификации;

- ГОСТ Р Защита информации. Идентификация и аутентификация. Управление идентификацией и аутентификацией.

Проект национального стандарта будет способствовать дальнейшему развитию комплекса стандартов в области идентификации и аутентификации объектов (субъектов) доступа в информационных системах.

Пересмотр, изменение или отмена действующих документов не требуется.

9 Перечень исходных документов и другие источники информации, использованные при разработке проекта стандарта, в том числе информацию об использовании документов, относящихся к объектам патентного или авторского права

При разработке проекта национального стандарта использовались следующие документы:

- Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

- Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;

- Приказ ФСТЭК России от 11.02.2013 № 17 «Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

- Приказ ФСТЭК России от 18.02.2013 № 21 «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

- Приказ ФСТЭК России от 14.03.2014 № 31 «Требования к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально

опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды»;

- Приказ ФСТЭК России от 25.12.2017 № 239 «Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации;

- ГОСТ Р 54581–2011/ISO/IEC/TR 15443-1:2005 Информационные технологии. Методы и средства обеспечения безопасности. Основы доверия к безопасности ИТ. Часть 1. Обзор и основы;

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

- ГОСТ Р 59383-2021 Информационные технологии. Методы и средства обеспечения безопасности. Основы управления доступом;

- Рекомендации по стандартизации Р 50.1.056-2005 Техническая защита информации. Основные термины и определения;

- ISO/IEC 29146:2016 Information technology – Security techniques – A framework for access management (Информационная технология. Методы и средства обеспечения безопасности. Основы управления доступом);

- NIST SP 800-63-3 Digital Identity Guidelines (Руководства по цифровой идентичности);

- NIST SP 800-63A Digital Identity Guidelines: Enrollment and Identity Proofing Requirements (Руководства по цифровой идентичности. Требования к регистрации и подтверждению идентичности);

- NIST SP 800-63B Digital Identity Guidelines: Authentication and Lifecycle Management (Руководства по цифровой идентичности. Аутентификация и управление жизненным циклом);

- ITSP.30.031 User authentication guidance for information technology systems (Руководство по аутентификации пользователей для систем информационных технологий);

- ITU-T X.1254 (09/2020) Cyberspace security – Identity management – Entity authentication assurance framework (Безопасность киберпространства. Управление идентичностью. Основы доверия аутентификации сущности).

При разработке проекта национального стандарта патенты не использовались.

10 Сведения о технических комитетах по стандартизации, в областях деятельности которых возможно пересечение с областью применения разрабатываемого проекта национального стандарта

Смежные технические комитеты отсутствуют.

11 Сведения о разработчике стандарта

Федеральная служба по техническому и экспортному контролю (ФСТЭК России).

Акционерное общество «Аладдин Р.Д.» (АО «Аладдин Р.Д.»),

129226, Москва, ул. Докукина, д.16 стр.1 эт.7, пом.1, ком.22,

Телефоны: +7 (495) 223-0001, +7 (495) 988-4640.

Факс: +7 (495) 646-0882

Электронная почта: standard@aladdin.ru.

Федеральное автономное учреждение «Государственный научно-исследовательский институт проблем технической защиты информации Федеральной службы по техническому и экспортному контролю» (ФАУ «ГНИИИ ПТЗИ ФСТЭК России»).

394020, г. Воронеж, ул. 9 Января, д. 280а.

Тел., факс: (473) 257-92-62.

E-mail: tk362@fstec.ru.

Доктор технических наук, профессор,
Заместитель генерального директора по
научной деятельности АО «Аладдин Р.Д.» А.Г. Сабанов