ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 59383— 2021

Информационные технологии

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Основы управления доступом

(ISO/IEC 29146:2016, NEQ)

Издание официальное

Москва
Стандартинформ
2021

Предисловие

1 РАЗРАБОТАН Федеральным государственным учреждением «Федеральный исследовательский центр «Информатика и управление» Российской академии наук» (ФИЦ ИУ РАН), Обществом с ограниченной ответственностью «Информационно-аналитический вычислительный центр» (ООО ИАВЦ) и Акционерным обществом «Аладдин Р.Д.» (АО «Аладдин Р.Д.»)

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 22 «Информационные технологии»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 20 мая 2021 г. № 414-ст

4 Настоящий стандарт разработан с учетом основных нормативных положений международного стандарта ИСО/МЭК 29146:2016 «Информационные технологии. Методы и средства обеспечения безопасности. Основы управления доступом» (ISO/IEC 29146:2016 «Information technology — Security techniques — A framework for access management», NEQ)

5 ВВЕДЕН ВПЕРВЫЕ

6 Федеральное агентство по техническому регулированию и метрологии не несет ответственности за патентную чистоту настоящего стандарта. Патентообладатель может заявить о своих правах и направить в национальный орган по стандартизации аргументированное предложение о внесении в настоящий стандарт поправки для указания информации о наличии в стандарте объектов патентного права и патентообладателе

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.gost.ru)

© Стандартинформ, оформление, 2021

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

Содержание

Введение

Управление безопасностью информации представляет собой сложную задачу, опирающуюся в основном на развитую отечественную нормативно-правовую базу [1], [2] и риск-ориентированный подход к защите информации, поддерживаемый рядом методов и средств обеспечения безопасности. Одной из задач обеспечения безопасности информации является разработка систем, которые реализуют политику управления доступом к информационным ресурсам организации [1]. В рамках управления безопасностью информации управление доступом играет ключевую роль в вопросе управления взаимодействием между получающими доступ сторонами: пользователями и ресурсами автоматизированных (информационных) систем. С развитием информационных сетей общего пользования информационные ресурсы могут размещаться в распределенных вычислительных сетях, которые предполагают наличие области единых правил управления доступом, включающей в себя политики, процессы, технологии, стандарты и типовые модели разграничения доступа.

Основы управления доступом представляют собой часть общих основ управления идентичностью и доступом. Управление доступом осуществляется после успешно выполненных идентификации и аутентификации субъектов доступа, претендующих получить доступ к информационным ресурсам.

Настоящий стандарт содержит описания концепций, участников, компонентов, эталонной архитектуры, функциональных требований и практических приемов управления доступом, а также описание архитектуры типовой системы управления доступом, реализуемой с применением нескольких моделей разграничения доступа, которые могут применяться разработчиками систем управления доступом в качестве методических материалов. Основное внимание в стандарте сосредоточено на задаче управления доступом для одной организации, при этом приведены некоторые предложения по управлению доступом объединения организаций, например территориально-распределенных предприятий и/или отраслевых структур.

Настоящий стандарт необходимо применять с учетом требований нормативных правовых актов и стандартов Российской Федерации в области защиты информации.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Информационные технологии

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Основы управления доступом

Information technology. Security techniques.
A framework for access management

Дата введения — 2021—11—30

1 Область применения

Настоящий стандарт определяет основы управления доступом и безопасного управления процессом доступа к информации и ресурсам средств информационно-коммуникационных технологий.

В настоящем стандарте приведены концепции, термины и определения, применимые для методов управления распределенным доступом в сетевой среде, представлены разъяснения, касающиеся взаимосвязанной архитектуры, компонентов и функций управления.

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

Описание характеристик и качества средств управления физическим доступом, задействованных в системах управления доступом, выходят за рамки применения настоящего стандарта.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

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

ГОСТ Р 59381 Информационные технологии. Методы и средства обеспечения безопасности. Основы управления идентичностью. Часть 1. Терминология и концепции

ГОСТ Р 59382 Информационные технологии. Методы и средства обеспечения безопасности. Основы управления идентичностью. Часть 3. Практические приемы

ГОСТ Р 59407 Информационные технологии. Методы и средства обеспечения безопасности. Базовая архитектура защиты персональных данных

ГОСТ Р ИСО/МЭК 27002 Информационные технологии. Методы и средства обеспечения безопасности. Свод норм и правил применения мер обеспечения информационной безопасности

Примечание — При пользовании настоящим стандартом целесообразно проверить действие ссылочных стандартов в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет или по ежегодному информационному указателю «Национальные стандарты», который опубликован по состоянию на 1 января текущего года, и по выпускам ежемесячного информационного указателя «Национальные стандарты» за текущий год. Если заменен ссылочный стандарт, на который дана недатированная ссылка, то рекомендуется использовать действующую версию этого стандарта с учетом всех внесенных в данную версию изменений. Если заменен ссылочный стандарт, на который дана датированная ссылка, то рекомендуется использовать версию этого стандарта с указанным выше годом утверждения (принятия). Если после утверждения настоящего стандарта в ссылочный стандарт, на который дана

Издание официальное

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 59381, а также следующие термины с соответствующими определениями:

3.1 **атрибут** (attribute): Характеристика, признак или свойство, используемые для описания и управления доступом к ресурсу.

Примечания

1 Правила предоставления доступа к ресурсу устанавливаются в политике управления доступом, которая определяет необходимые атрибуты для разрешения доступа субъекта к ресурсу для определенной операции.

2 Примерами атрибутов могут быть атрибуты субъекта, атрибуты ресурса, атрибуты окружения и иные атрибуты, используемые для управления доступом, как определено в политике управления доступом.

3.2 **конечная точка** (endpoint): Сервис принятия решения в системе управления доступом, в котором осуществляется функция управления доступом.

Примечания

1 Возможны следующие различные виды конечных точек:

- сервис принятия решения по результату аутентификации субъекта доступа;
- сервис принятия решения по авторизации субъекта доступа;
- сервис обнаружения конечных точек, осуществляющий поиск и определяющий местонахождение конечных точек;
- сервис начального обнаружения конечных точек, используемый в начале взаимодействия субъекта с системой управления доступом.

2 Сервисы обнаружения конечных точек обычно используются в распределенных сетевых системах.

3.3 **привилегия** (privilege): Метка разрешения для субъекта на доступ к ресурсу.

Примечания

1 Привилегия является необходимым, но не достаточным условием для доступа. Доступ осуществляется, когда запрос доступа удовлетворяется в соответствии с принятой политикой управления доступом. Политика управления доступом основывается на привилегиях и может включать в себя другие факторы среды (например, время дня, местоположение и т. д.).

2 Привилегии имеют форму данных, представляемых или получаемых субъектом. Эти данные используются точкой принятия решений по политике для разрешения или отказа в осуществлении операции, которую субъект хочет осуществить с ресурсом.

3 Ресурс может иметь несколько различных ассоциированных с ним привилегий, которые соответствуют определенным уровням доступа. Например, ресурс данных может иметь права на чтение, запись, выполнение и удаление, доступные для назначения субъектам. Запрос субъекта на доступ к ресурсу может быть разрешен для некоторых уровней доступа, но запрещен для других уровней, в зависимости от уровня запрашиваемого доступа и привилегий ресурса, назначенных субъекту.

4 Право доступа определяет возможное действие, которое субъект может выполнять с ресурсом.

3.4 **принцип необходимого знания** (need-to-know). Цель безопасности, состоящая в поддержании доступа субъекта к информационным ресурсам на минимальном уровне, необходимом для выполнения своих функций делающим запрос пользователем.

Примечания

1 Принцип необходимого знания санкционируется по усмотрению владельца ресурса.

2 Принцип необходимого наличия — это цель безопасности запрашивающей стороны для выполнения конкретных задач, которые могут ограничиваться по усмотрению владельца ресурса.

3.5 **разграничение доступа** (access control): Разрешение или отказ в осуществлении операции с ресурсом.

Примечания

1 Основной целью разграничения доступа является предотвращение несанкционированного доступа к информации или использование информационных ресурсов на основе бизнес-требований и требований безопасности, т. е. применение политик доступа к конкретным запросам.

2 При получении запроса от аутентифицированного субъекта владелец ресурса разрешает (или не разрешает) доступ в соответствии с политикой доступа и привилегиями субъекта.

3.6 **реализация, ориентированная на организацию** (enterprise centric implementation): Управление доступом, проводимое под контролем точки принятия решений по политике.

3.7 **реализация, ориентированная на субъекта** (subject centric implementation): Управление доступом, реализованное как компонентные сервисы, которые вызываются субъектом с целью получения средств, признаваемых точкой соблюдения политики, для получения доступа к ресурсу.

Примечание — Компонентные сервисы могут включать в себя сервис точки принятия решений по политике, сервис точки соблюдения политики и соответствующие сервисы обнаружения, дающие возможность субъекту определять местоположение и контактировать с сервисами управления доступом.

3.8 **ресурс** (resource): Физический, сетевой или любой информационный актив, к которому может быть получен доступ субъектом.

3.9 **роль** (role): Название, данное определенной совокупности функций системы, которые могут выполняться многими сущностями.

Примечания

1 Название обычно описывает функциональные возможности.

2 Сущности могут быть, но не обязательно являются людьми.

3 Роли реализуются совокупностью атрибутов привилегий для предоставления необходимого доступа к информационным ресурсам или объектам.

4 Назначенные на роль субъекты наследуют связанные с ролью привилегии доступа. При операционном использовании субъектам следует аутентифицироваться в качестве членов ролевой группы, прежде чем им будет разрешено выполнять функции роли.

3.10 **сервис токенов безопасности** (security token service): Сервис, создающий, подписывающий, осуществляющий замену и выпуск токенов доступа на основе решений, принимаемых точкой принятия решений по политике.

Примечание — Этот сервис может быть разбит на отдельные компоненты.

3.11 **субъект** (subject): Сущность, запрашивающая доступ к ресурсу, находящемуся под контролем системы управления доступом.

3.12 **токен доступа** (access token): Доверенный объект, инкапсулирующий полномочия субъекта для получения доступа к ресурсу.

Примечания

1 Токен доступа выпускается точкой принятия решений по политике и используется точкой соблюдения политики для ресурса.

2 Токен доступа может содержать информацию о разрешении доступа для получения субъектом доступа к ресурсу и идентификационную информацию для источника решения об авторизации.

3 Токен доступа может содержать информацию, позволяющую осуществить проверку его достоверности.

4 Токен доступа может иметь физическую или виртуальную форму.

3.13 **точка администрирования политики** (policy administration point): Сервис, осуществляющий администрирование политики авторизации доступа.

Примечание — Атрибуты могут включать в себя привилегии/разрешения, связанные с ресурсом, субъектом и средой.

3.14 **точка информирования по политике** (policy information point): Сервис, выполняющий функции источника атрибутов, которые используются точкой принятия решений по политике для принятия решений об авторизации.

Примечание — Атрибуты могут включать в себя привилегии/разрешения, связанные с ресурсом, субъектом и средой.

3.15 **точка принятия решений по политике** (policy decision point): Сервис, реализующий политику разграничения доступа для принятия решений по запросам сущностей о доступе к ресурсам и предоставления решений об авторизации, используемых точкой соблюдения политики.

Примечания

1 Решения об авторизации используются точкой соблюдения политики для управления доступом к ресурсу. Решения об авторизации могут сообщаться посредством использования токена доступа.

2 Точка принятия решений по политике также осуществляет аудит решений в контрольном журнале и может инициировать предупреждения.

3 Этот термин соответствует функции принятия решений о доступе, приведенной в [3]. Предполагается, что эта функция располагается в сети субъекта и может находиться в сети в виде соответствующей точки соблюдения политики.

3.16 **точка выполнения политики** (policy enforcement point): Сервис, обеспечивающий выполнение решения о доступе точки принятия решений по политике.

Примечания

1 Точка выполнения политики получает решения об авторизации, принятые точкой принятия решений по политике, и реализует их для осуществления разграничения доступа сущностей к ресурсам. Решение об авторизации может быть получено в форме токена доступа, представляемого субъектом при осуществлении запроса о доступе.

2 Этот термин соответствует функции обеспечения осуществления доступа, приведенной в [3]. Предполагается, что эта функция располагается в сети субъекта и может находиться в сети в виде соответствующей точки принятия решений по политике.

3.17 **управление доступом** (access management): Совокупность процессов разграничения доступа для ряда ресурсов.

4 Основные концепции

4.1 Модель управления доступом к ресурсам

4.1.1 Общий обзор

Концептуально последовательность предоставления доступа к ресурсу выглядит следующим образом:

- перед предоставлением доступа к ресурсу необходима аутентификация субъекта. Однако аутентификация является отдельной функцией, обычно реализуемой на сеансовой основе, а не для каждого запроса доступа;
- решение об авторизации, разрешающее доступ или отказывающее в доступе к ресурсу, принимается на основе политики; для передачи результата решения выпускается токен доступа;
- на основе результата решения осуществляется авторизация для ресурса и предоставляется доступ к ресурсу.

Последовательность действий в модели управления доступом приведена на рисунке 1. Субъект и ресурс изображены в виде окружностей, а концептуальные функции изображены в виде прямоугольников.

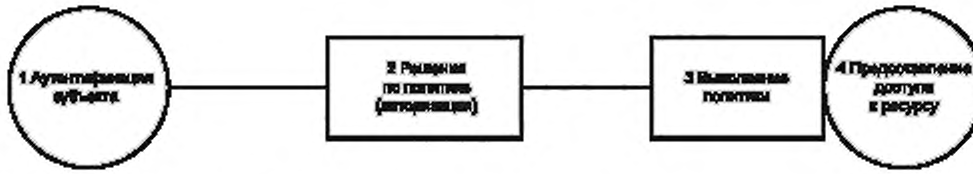

Рисунок 1 — Последовательность действий в модели управления доступом

Для цели предоставления доступа ресурс характеризуется следующими аспектами:

- идентификатором для конкретного ресурса либо для класса ресурсов;
- одним или несколькими режимами доступа;

- совокупностью атрибутов, связанных с режимами доступа и другими критериями доступа, как определено в политике управления доступом.

Система управления доступом отвечает за администрирование и функционирование разрешений на доступ. Полномочия поддерживаются административной деятельностью, которая назначает и поддерживает атрибуты ресурсов и привилегии субъекта в соответствии с политикой управления доступом.

Ресурсы в системах обычно являются динамичными. Они проходят жизненный цикл от создания до уничтожения, и этот процесс является непрерывным.

Ресурсы постоянно создаются, обновляются и уничтожаются.

Ресурсам должны быть присвоены атрибуты доступа (как правило во время создания), которые будут использоваться системой управления доступом для управления доступом субъектов к ресурсам. [Это осуществляется путем предварительного определения общепризнанных типов ресурсов с соответствующими образцами атрибутов доступа. При создании ресурса известного типа он наследует атрибуты доступа соответствующего образца].

Ресурсами владеет сторона, которая может быть физическим лицом или организацией. Владелец часто, но не всегда, является создателем ресурса, и владение ресурсом может меняться в течение срока службы ресурса.

4.1.2 Взаимосвязь между системой управления идентификационными данными и системой управления доступом

В приведенной в настоящем стандарте модели управления доступом субъект аутентифицируется с помощью системы управления идентификационными данными, как указано в [4]. Затем аутентифицированный субъект запрашивает доступ, используя систему управления доступом. Система управления доступом определяет, следует ли авторизовать субъекта для доступа к ресурсу. Авторизация субъекта включает в себя два различных вида деятельности:

- предварительное присвоение субъектам привилегий доступа к ресурсам;
- предоставление субъектам доступа к ресурсам при операционном использовании.

Взаимосвязь между системой управления идентификационными данными и системой управления доступом приведена на рисунке 2.

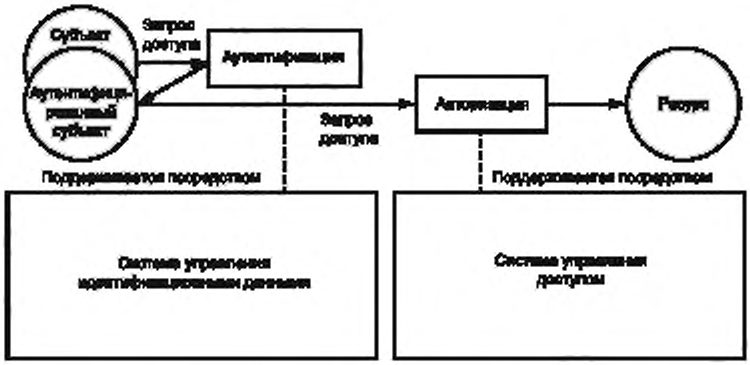

Рисунок 2 — Взаимосвязь между системой управления идентификационными данными и системой управления доступом

Аутентификация поддерживается системой управления идентификационными данными. В системе управления доступом, использующей модель управления доступом на основе идентификационных данных, идентификационные данные являются основой для присвоения субъектам привилегий доступа к ресурсам и авторизации запросов доступа субъектов к ресурсам при операционном использовании.

Примечание — Предоставление доступа к ресурсу может требовать минимального установленного уровня доверия к аутентификации для субъекта, который зависит от риска ресурса. Требуемый уровень доверия зависит от связанного с идентификационными данными риска, относящегося к ресурсу, к которому нужно получить доступ. Дополнительная информация об уровне доверия к аутентификации содержится в ГОСТ Р 58833.

Авторизацию обеспечивает система управления доступом, которая поддерживает управление информацией о доступе.

Практические приемы реализации систем управления доступом могут варьироваться в зависимости от используемой архитектуры и модели управления доступом, например:

- в случае реализации системы управления доступом как системы веб-сервисов, субъект может запросить доступ к ресурсу без предварительной аутентификации. В этом случае система управления доступом перенаправит субъекта, чтобы он запросил систему управления идентификационными данными о положительном результате аутентификации;
- в случае применения модели управления доступом на основе атрибутов имеется возможность не требовать аутентификации для субъекта. В этом случае анонимному субъекту может быть разрешено перейти непосредственно в систему управления доступом, и решение об авторизации будет принято на основе учетных данных, которые могут быть проверены, чтобы доказать, что субъект обладает заявленными атрибутами.

4.1.3 Характеристики безопасности метода доступа

Необходимо рассмотреть аспекты безопасности реализации систем управления доступом и процессов, особенно в случае использования объединенных (междоменных) архитектур.

По соображениям безопасности может требоваться проверка целостности запроса доступа, прежде чем запрос будет обрабатываться системой управления доступом.

В случаях, когда каналы связи являются надежными, например частные соединения внутри организации, дополнительная защита может не требоваться. Однако в случаях, когда каналы связи проходят через общедоступные сети или другие незащищенные каналы, необходимо предусмотреть меры по обеспечению целостности и конфиденциальности запросов доступа и связанных с ними данных как самого запроса доступа (привилегии, аутентификационные данные субъекта, ресурс, запрашиваемая операция и т. д.), так и данных, отправленных ресурсу или полученных от него в течение периода доступа.

Существуют два подхода к установлению безопасного канала связи между субъектом и системой управления доступом. Представленные ниже подходы учитывают время, когда будет установлен безопасный канал связи:

- безопасный канал связи может быть установлен до передачи привилегий или данных, которые будут использоваться для получения привилегий (например, путем создания сеанса с протоколом защиты безопасности транспортного уровня (TLS) с поддерживающим ресурс сервером);
- безопасный канал связи может быть установлен после успешной передачи привилегий или данных, которые использовались для аутентификации идентификатора субъекта.

В последнем случае безопасный канал связи устанавливается после успешного аутентификационного обмена либо после успешного приема токена доступа; ключи целостности и конфиденциальности выводят из аутентификационного обмена или получают из информации, содержащейся в токене доступа, или из информации, связанной с токеном доступа. Затем через безопасный канал связи может осуществляться передача данных операции, запрашиваемой у ресурса.

4.2 Взаимосвязь между управлением логическим и физическим доступом

В настоящем стандарте основное внимание уделяется управлению логическим доступом. Как правило, управление логическим доступом интегрировано с управлением физическим доступом.

Логический доступ к ресурсу в автоматизированной (информационной) системе организации должен поддерживаться защищенной физической инфраструктурой, обеспечивающей эффективный набор мер защиты и ограничений на действия субъектов доступа.

Для логического доступа к ресурсу, размещаемому с привлечением внешнего сервиса, внешний сервис должен отвечать за реализованное в нем управление физическим и логическим доступом, чтобы субъект мог ему доверять.

4.3 Функции и процессы системы управления доступом

4.3.1 Общий обзор

Система управления доступом обеспечивает соблюдение политики разграничения доступа и выполняет две основные операционные функции:

- присвоение субъектам привилегий доступа к ресурсам до начала операционного использования; альтернативным образом присвоение привилегий доступа атрибутам (как в модели разграничения доступа на основе идентификационных данных, см. 4.3.2), а затем присвоение атрибутов субъектам, которые наследуют соответствующие привилегии доступа;

- использование этих привилегий (вместе с другой информацией, где это уместно) для разграничения доступа субъектов к ресурсам системы при операционном использовании.

Кроме того, система управления доступом обеспечивает административные функции для поддержки основных функций, включая:

- управление политиками;
- управление связанными с политиками атрибутами доступа;
- управление мониторингом и учетом (аудитом).

Политика доступа к ресурсам должна реализовывать следующие принципы:

- установление атрибутов доступа на основе принципа «необходимого знания»;
- минимизацию доступа к данным с целью ограничения доступа только строго необходимыми данными и сведения к минимуму риска утечки и раскрытия данных;
- отделение и обеспечение защиты чувствительных данных;
- обеспечение защиты персональных данных;
- применение многофакторной аутентификации в случае критичности и чувствительности ресурса, к которому предоставляется доступ.

4.3.2 Политика управления доступом

Система управления доступом обеспечивает соблюдение политики разграничения доступа. Существует ряд моделей разграничения доступа (см. приложение А). В настоящем стандарте содержится описание моделей разграничения доступа, которые являются достаточно гибкими, чтобы быть пригодными для использования и в централизованной, и в распределенной сетевой среде:

- разграничение доступа на основе идентификационных данных (identity-based access control);
- разграничение доступа на основе ролей (role-based access control);
- разграничение доступа на основе атрибутов (attribute-based access control).

Политика разграничения доступа должна быть описана на естественном языке или посредством другого пригодного представления, например формального языка, чтобы выражать цели разграничения доступа к ресурсам, методы и процессы осуществления контроля и любые требования мониторинга, аудита и других неосновных функций.

В организации может существовать ряд политик разграничения доступа. Как правило, доступ к группе ресурсов одной технологии может быть осуществлен под контролем точки принятия решений, отвечающей одной политике, в то время как доступ к другой группе ресурсов, разработанных с использованием другой технологии, будет осуществлен под контролем другой точки принятия решений, отвечающей второй политике разграничения доступа. Рекомендуется, чтобы обе точки принятия решений могли соответствовать одной и той же политике разграничения доступа.

В случаях, когда в организации действует несколько систем управления доступом и они должны быть интегрированы в единую систему, необходимо устранить разногласия политик, выработать и документально оформить общую политику разграничения доступа. Альтернативным подходом может быть интеграция систем в виде внутриорганизационного объединения; в этом случае следует учитывать соображения и требования, приведенные в 4.3.8.

Разграничение доступа обеспечивается посредством механизмов разрешения или отказа в выполнении операций с ресурсами на основе политики разграничения доступа.

Решения об авторизации принимаются на основе оценивания привилегий и атрибутов субъекта относительно правил доступа, установленных для соответствующего ресурса. Правила могут включать в себя атрибуты среды, такие как время суток и местоположение, из которых делается запрос. Например, все операции с ресурсом могут быть запрещены в период времени между 21:00 и 7:00.

Если применяется мандатное разграничение доступа, правило обязательно будет общим для совокупности ресурсов. Например, субъекты должны иметь допуск к работе для осуществления любой операции, которую они хотели бы выполнить в отношении данного набора ресурсов.

Примечание — Так как последовательно может применяться несколько правил, порядок их применения может влиять на эффективность процесса принятия решения. Однако оптимальное упорядочение будет зависеть от относительной вероятности принятия решений о предоставлении/отказе в доступе при операционном использовании.

Отдельные правила могут быть реализованы с помощью матрицы разграничения доступа, связанной с каждым ресурсом, которая содержит одну или несколько записей.

Каждая запись будет определять условие(я), которое(ые) необходимо выполнить субъекту для осуществления одной или нескольких операций с ресурсом. Главное условие для выполнения состоит в том, что субъект должен обладать некоторой(ыми) привилегией(ями).

Разграничение доступа на основе атрибутов представляет собой наиболее общий случай, когда управление доступом основано на определяемых системой управления доступом атрибутах, которыми обладают субъекты. Разграничение доступа на основе идентификационных данных, на основе псевдонимов и на основе ролей представляют собой частные случаи разграничения доступа на основе атрибутов, где атрибутами соответственно являются идентификационные данные, псевдонимы и роли. Эти четыре модели разграничения доступа могут быть реализованы с использованием списков разграничения доступа.

Когда субъект представляет свидетельство возможностей (при разграничении доступа на основе возможностей) для авторизации, необходимо проверить, что свидетельство возможностей в качестве токена доступа является эффективным для данной операции.

В системах управления доступом, включающих в себя более чем одну модель разграничения доступа, следует позаботиться об обеспечении уверенности в том, что политики, определяющие доступ субъектов к ресурсам, не приводят к конфликтным решениям о доступе для одного и того же субъекта по разным вариантам доступа: точка администрирования политики должна быть способна управлять доступом, реализованным на основе различных моделей разграничения доступа.

Политика управления доступом должна иметь следующие характеристики:

- основываться на требованиях политики, являющихся общими для существующих требуемых моделей разграничения доступа, при обеспечении защиты информации в соответствии с бизнес-требованиями и по соображениям соблюдения правовых, нормативных требований и прав интеллектуальной собственности;
- содержать иерархию политик, основанную на общей политике, из которой могут определяться правила разграничения доступа, применяемые к субъектам доступа с одинаковыми характеристиками;
- описывать атрибуты, поддерживающие определенную классификацию. Такая классификация позволит обеспечить совместимость политик и соответствие среди различных организаций;
- описывать процедуры предоставления и управления привилегиями, процесс разграничения доступа и обработку особых ситуаций.

4.3.3 Управление привилегиями (правами доступа)

Требования управления привилегиями определяются политикой разграничения доступа, как приведено в 4.3.2.

В соответствии с политикой разграничения доступа на основе идентификационных данных управление привилегиями осуществляется на основе идентификационных данных субъекта. Политика разграничения доступа на основе идентификационных данных использует такие механизмы, как списки управления доступом для определения идентификационных данных тех, кому разрешен доступ к ресурсу, и типов операций с ресурсом, которые им разрешено выполнять. В модели разграничения доступа на основе идентификационных данных предоставление субъекту привилегий доступа к ресурсу производится до любого запроса субъекта о доступе, а идентификационные данные субъекта и привилегии доступа добавляются к соответствующему списку разграничения доступа для ресурса.

Если идентификационные данные аутентифицированного субъекта совпадают с идентификационными данными, зафиксированными в соответствующем списке управления доступом, субъекту предоставляют доступ к ресурсу в соответствии с его привилегиями доступа. Каждый ресурс имеет соответствующий список разграничения доступа, где фиксируются привилегии доступа для субъектов, которым разрешен доступ к ресурсу. В модели разграничения доступа на основе идентификационных данных решение об авторизации принимается до любого конкретного запроса доступа и приводит к добавлению субъекта и привилегий доступа субъекта в соответствующий(е) список (списки) разграничения доступа для ресурса.

При разграничении доступа на основе ролей каждому субъекту присваивается роль (или роли) и это фиксируется в учетной записи для данного субъекта. Решение об авторизации принимается на основе привилегий доступа, присвоенных соответствующей роли в системе разграничения доступа. В модели разграничения доступа на основе ролей привилегии присваиваются ролям, а не субъектам. Роли между субъектами распределяются с помощью отдельной процедуры. Это также влияет на процесс авторизации при запросе доступа к ресурсам, который является двухэтапным процессом в модели разграничения доступа на основе ролей:

- авторизация запроса доступа для роли;
- аутентификация субъекта как члена ролевой группы.

При разграничении доступа на основе атрибутов субъектам присваиваются связанные с политикой атрибуты доступа. Решения об авторизации основываются на атрибутах, которыми обладают

субъекты. Субъект может получать доступ к ресурсам как член группы, обладатель атрибутов или как индивидуум. При этом в системе управления доступом могут одновременно существовать способы управления доступом на основе ролей, атрибутов и идентификационных данных.

Управление привилегиями включает в себя следующие виды деятельности:

- создание набора привилегий, используемых для обозначения и ограничения типов операций, которые могут выполняться с ресурсами;
- установление правил, определяющих присвоение привилегий в соответствии с политикой разграничения доступа и используемой способом управления доступом, например присвоение привилегий идентификационным данным, ролям, возможностям или иным определенным атрибутам;
- обновление и аннулирование привилегий и идентификационных атрибутов.

Реализация политики разграничения доступа происходит в результате присвоения привилегий доступа к ресурсам, субъектам, ролям, группам и т. д. Привилегии следует присваивать по принципу минимального «необходимого знания», предоставляющего самый низкий уровень привилегий в соответствии с необходимостью субъекта доступа осуществлять соответствующую деятельность.

Примечание — Привилегии могут присваиваться субъектам доступа, ассоциированным с физическими лицами, и субъектам доступа, не ассоциированным с физическими лицами. Например, когда в сеть добавляется устройство или сервис, им могут присваиваться привилегии доступа к ресурсам.

4.3.4 Управление информацией об атрибутах, связанной с политикой доступа

Управление информацией при установке привилегий атрибутам относится к функциям администратора, как приведено в 5.1.

Такого рода информация характеризуется следующим:

- ее получают из различных источников, включая связанные с атрибутами органы управления, ресурсы и среду;
- управление ею осуществляется через точку администрирования политики;
- она хранится в точке информирования по политике.

Результирующая информация предоставляется точке принятия решений по политике разграничения доступа к ресурсам.

Управление информацией об атрибутах в системе управления доступом осуществляется в соответствии с описанной ранее политикой разграничения доступа.

В случае использования модели разграничения доступа на основе атрибутов политика формулируется в терминах атрибутов, которые используются для управления доступом к ресурсам, и исходя из того, как атрибуты соответствуют привилегиям доступа к ресурсам. Для модели разграничения доступа на основе ролей политика определяет, как привилегии доступа к ресурсам присваиваются различным ролям.

В соответствии с политикой разграничения доступа управление атрибутами осуществляют владельцы ресурсов, тогда как в рамках политики мандатного управления доступом управление дополнительными атрибутами осуществляют специалисты по реализации политики.

В случае использования модели разграничения доступа на основе псевдонимов используются такие механизмы, как списки управления доступом, содержащие псевдонимы субъектов, которым разрешен доступ к ресурсу, вместе с разрешениями на доступ субъекта к ресурсу. Если субъект представляется псевдонимом, совпадающим с тем, который содержится в списке управления доступом, субъекту может быть предоставлено право осуществления операции с ресурсом с учетом его разрешений и любых других проверок, которые могут быть применены.

В модели разграничения доступа на основе идентификационных данных применяется сходный механизм, в котором вместо псевдонимов используются идентификационные данные.

В модели разграничения доступа на основе ролей применяется аналогичный механизм, в котором вместо псевдонимов используются роли.

В модели разграничения доступа на основе атрибутов применяется сходный механизм, в котором вместо псевдонимов используются атрибуты (например, членство в группах).

Все вышеуказанные модели разграничения доступа могут одновременно существовать в системе управления доступом.

Модель разграничения доступа на основе возможностей использует механизмы, в которых представленная субъектом возможность должна: во-первых, сопоставляться с идентификатором ресурса и операцией, осуществляемой с ресурсом; во-вторых, содержание возможности должно также сопоставляться с идентификатором признанного органа и соответствующими операциями, разрешенными для

этого органа. Если эти условия выполнимы, то субъекту может быть предоставлено право осуществления операции с ресурсом до следующих проверок, которые могут применяться.

Более подробная информация о моделях разграничения доступа содержится в приложении А.

4.3.5 Авторизация

Базовая авторизация происходит во время операционного этапа и осуществляется в точке принятия решений по политике в соответствии с политикой разграничения доступа. Это действие поддерживается управлением со стороны администратора.

При определенных условиях авторизация может предоставляться делегату субъекта (выполняться авторизация делегированного доступа). Делегатом может быть физическое лицо, веб-сервер, клиентское приложение, работающее под контролем субъекта. Делегат обычно наследует привилегии доступа субъекта и должен быть аутентифицирован так же, как субъект или эквивалентным образом. Сценарий делегирования представлен на рисунке 3.

Примечание — Это вариант использования, поддерживаемый протоколом OAuth. В данном случае решение об авторизации принимает владелец ресурса в режиме реального времени или с учетом заранее зарегистрированной политики, установленной владельцем ресурса. Если субъект является делегатом, то система управления доступом может определить решение об авторизации на основе учетных данных, которыми уже обладает делегат. Если субъект не является делегатом, необходимо связаться с владельцем ресурса, чтобы узнать, разрешено ли этому неавторизованному лицу получить доступ к ресурсу.

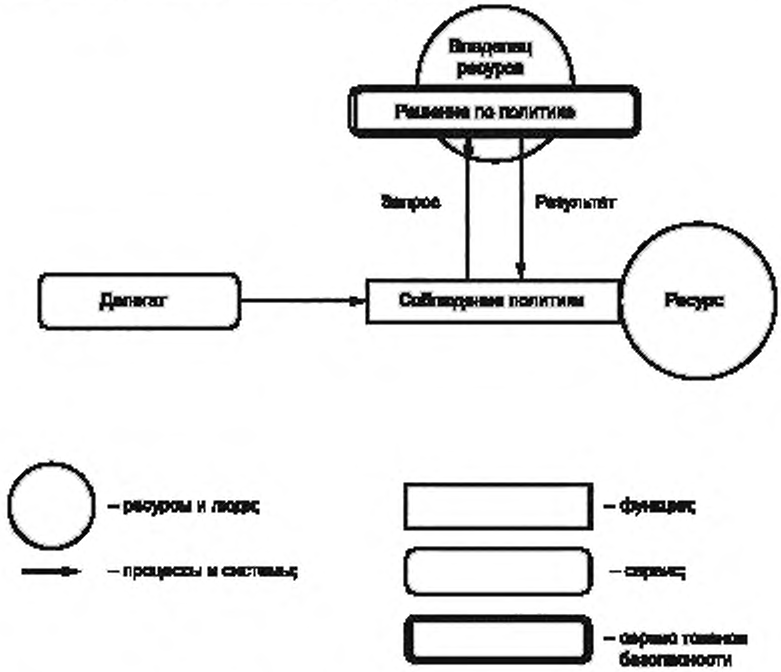

Рисунок 3 — Авторизация делегированного доступа

4.3.6 Управление мониторингом

Действия, связанные с управлением доступом, должны контролироваться в целях обеспечения соответствия, регулирования и проведения расследований.

Система управления доступом должна обеспечивать проверяемые возможности мониторинга и ведения учета для целей соблюдения нормативных требований, ответственности и расследования инцидентов.

Система управления доступом должна предоставлять возможности мониторинга операций с ресурсами, которые пытаются осуществить субъекты, и учетом того, были ли эти операции разрешены или в них было отказано.

В контрольном журнале должны быть зафиксированы следующие параметры:

- идентификатор ресурса;
- операция с ресурсом, осуществление которой запрашивает субъект;
- решение (т. е. разрешение или отказ) вместе с обоснованием;
- время предоставления доступа или отказа в нем;
- привилегии или атрибуты субъекта, как уместно;
- любая информация, которая может прямо или косвенно идентифицировать субъекта.

Кроме того, система управлением доступом должна предоставлять инструменты для простого построения аудиторских отчетов с использованием фильтров, основанных на предыдущих шести параметрах, которые можно найти в журнале аудита.

Владелец ресурса должен определять условия доступа, которые будут использоваться точкой принятия решений по политике для принятия решения о предоставлении субъекту доступа к ресурсу.

4.3.7 Управление предупреждениями

Как правило, целью предупреждений является оповещение аудиторов управления доступом о ненормальных условиях эксплуатации. Такие ситуации должны быть определены в политике управления доступом вместе с процедурами обработки и в процедурах урегулирования, реализованных в управлении мониторингом. Ненормальные ситуации могут включать в себя попытки доступа к ресурсам неавторизованных субъектов. Аварийные условия определяются таким образом, чтобы их можно было распознать при оперативном использовании и принять соответствующие меры. При возникновении аварийных ситуаций они должны быть записаны в журнал аудита для последующего анализа.

Предупреждения могут быть инициированы одним или несколькими условиями, которые могут относиться к следующему:

- идентификатору ресурса;
- операции с ресурсом, осуществление которой запрашивает субъект;
- решению (т. е. разрешению или отказу) вместе с обоснованием;
- времени предоставления доступа или отказа в нем;
- привилегии или атрибутам субъекта, если уместно;
- любой информации, которая может прямо или косвенно идентифицировать субъекта.

После инициирования предупреждения может быть проведено дальнейшее расследование с использованием журнала аудита, созданного для мониторинга событий.

4.3.8 Управление объединенным доступом

Управление объединенными идентификационными данными и управление доступом требуется в случаях, когда аутентифицированный субъект из одной организации пытается получить доступ к ресурсу другой организации. Существует несколько способов управления объединенными идентификационными данными, описание которых содержится в ГОСТ Р 59382 и [4]. Пример управления объединенным доступом приведен на рисунке 4. Предполагая, что субъект может аутентифицироваться в объединенной модели, требования управления объединенным доступом реализуются членами объединения в соответствии с совместными доверительными отношениями и общими политиками, согласованными участвующими в сообществе организациями.

а) Субъект должен аутентифицироваться у полномочного органа своей организации;

б) организация субъекта предоставляет утверждение, относящееся к управлению доступом, организации-владельцу ресурса, которое подтверждает действительность аутентификации субъекта и предоставляет контекст аутентификации и согласованные атрибуты доступа, включая привилегии разграничения доступа на основе атрибутов или на основе ролей;

в) организация-владелец ресурса принимает утверждение и рассматривает атрибуты по отношению к политикам управления доступом владельца информационных ресурсов;

г) владелец ресурса данных разрешает субъекту доступ к ресурсу или запрещает доступ, и уведомляет субъекта;

д) все уполномоченные участники фиксируют события, связанные с разграничением доступа.

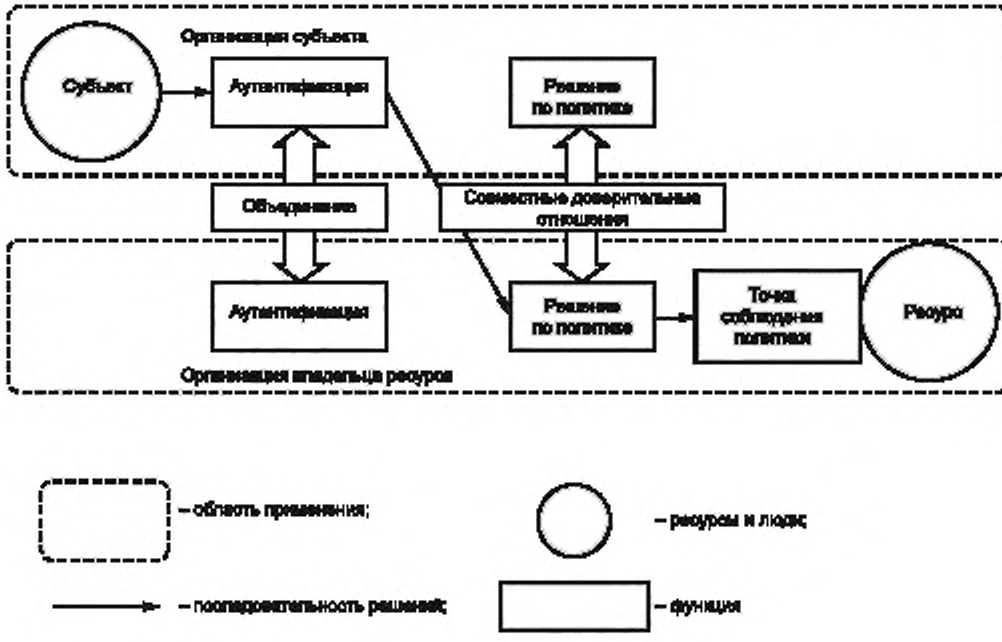

Рисунок 4 — Управление объединенным доступом

Совместные доверительные отношения для разграничения доступа в объединении должны:

- основываться на согласованных требованиях о защите информации объединения с соблюдением требований нормативно-правовых актов и требований к защите интеллектуальной собственности;
- содержать общие элементы политики, из которых могут быть определены правила разграничения доступа и классификация их реализации;
- определять токены доступа (атрибуты, разрешения и т. д.), которые могут приниматься во всем объединении, чтобы способствовать установлению доверительных отношений между членами объединения.

5 Эталонная архитектура

5.1 Общий обзор

Представленные в разделе 4 компоненты определяют эталонную архитектуру системы управления доступом (рисунок 5).

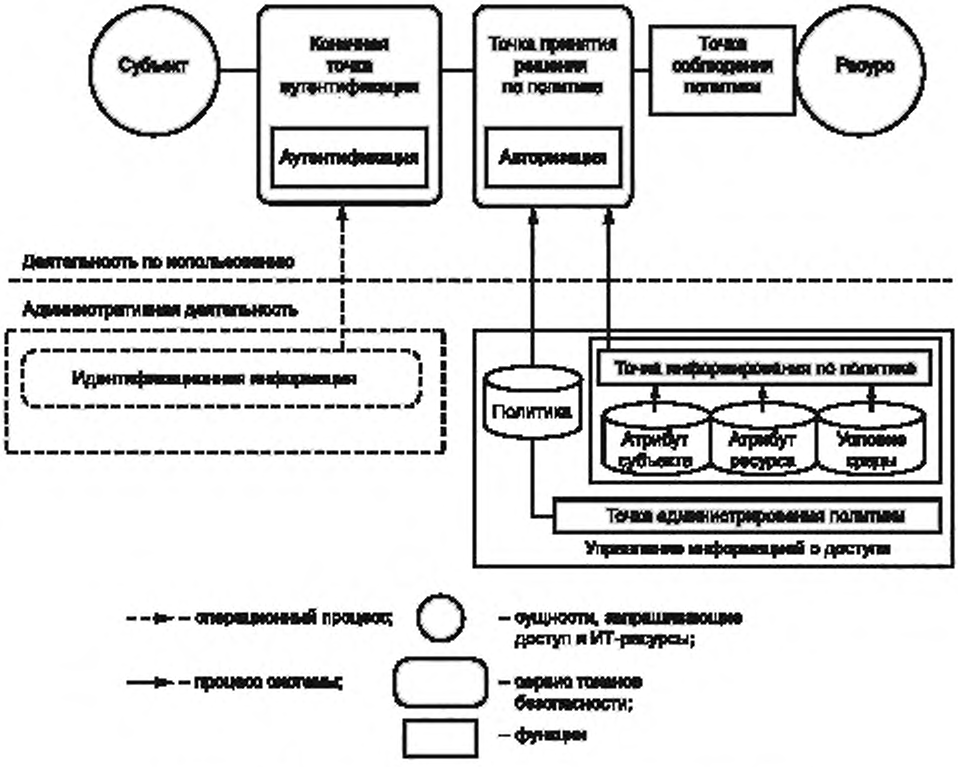

Рисунок 5 — Эталонная архитектура системы управления доступом

5.2 Основные компоненты системы управления доступом

5.2.1 Конечная точка аутентификации

Конечная точка аутентификации обеспечивает аутентификацию субъекта для использования полученного результата точкой принятия решений по политике при принятии решений о доступе субъектов к ресурсам.

5.2.2 Точка принятия решений по политике

Точка принятия решений по политике принимает решения об авторизации для разрешения или отказа в доступе к ресурсу и передает эти решения точке соблюдения политики для реализации.

Точка принятия решений по политике реализует политику разграничения доступа или набор политик для ресурса. На основе определенного набора политик точка принятия решений по политике решает, может ли субъект получить доступ к ресурсу.

В некоторых случаях политика создается в режиме реального времени через интерфейс с владельцем ресурса. В ориентированных на организацию реализациях разграничения доступа этот сервис часто называют «конечной точкой авторизации пользователя».

Точка принятия решений по политике поддерживается точкой информирования по политике.

5.2.3 Точка информирования по политике

Этот компонент выполняет функции источника значений атрибутов (например, ресурс, субъект, условие среды), которые используются точкой принятия решений по политике для принятия решения об авторизации.

5.2.4 Точка администрирования политики

Этот компонент предоставляет интерфейс для администрирования набора политик и взаимосвязанной информации в точке информирования по политике. Их администрирование может включать в себя конфигурирование, тестирование, отладку и хранение. Для администрирования набора политик

разграничения доступа необходим прикладной программируемый интерфейс для точки администрирования политики.

Политика или набор политик могут основываться на разграничении доступа на основе ролей или на основе атрибутов, или на любой другой модели разграничения доступа, или их комбинации.

Политика на естественном языке должна быть переведена в эквивалентное цифровое представление политики, которое использует точка принятия решений по политике для определения своих решений об авторизации.

5.2.5 Точка соблюдения политики

В точке соблюдения политики принимается решение об авторизованном доступе к ресурсам и осуществляется защита ресурса от неавторизованного доступа.

Точка соблюдения политики перехватывает запрос субъекта о доступе к ресурсу и перенаправляет его к решению об авторизации, которое принимается точкой принятия решений по политике.

5.3 Дополнительные сервисные компоненты

5.3.1 Общие положения

При реализации логического представления могут дополнительно вводиться некоторые сервисы.

5.3.2 Реализация, ориентированная на субъекта

5.3.2.1 Обзор

На рисунке 6 приведен случай реализации, где решающую роль играет субъект.

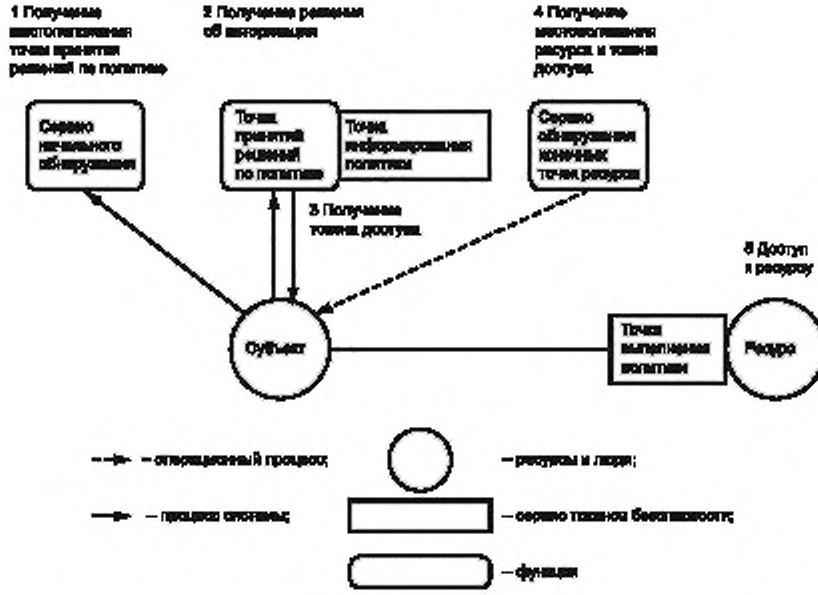

Рисунок 6 — Взаимодействие компонентных сервисов в реализации, ориентированной на субъекта

5.3.2.2 Сервис начального обнаружения конечных точек

В некоторых вариантах использования портальный сервис может реализовываться таким образом, что он осуществляет начальное обнаружение в начале взаимодействия субъекта, чтобы направлять субъекта. Как правило, сервисом начального обнаружения является конечная точка аутентификации.

Примечание — В настоящем стандарте сервис аутентификации субъекта не описывается. Описание сервиса содержится в ГОСТ Р 59381, а также приведено в [4] и [5].

5.3.2.3 Сервис токенов безопасности

На основании решения, принятого точкой принятия решений по политике, сервис токенов безопасности может создавать, подписывать, осуществлять замену и выпуск токенов доступа.

Примечание — Описание токенов доступа содержится в ГОСТ Р 58833.

Сервис токенов безопасности может составлять часть функций других компонентов системы управления доступом.

5.3.2.4 Сервис обнаружения ресурсов

Сервис обнаружения ресурсов предоставляет информацию о местоположении ресурсов, которыми управляет система управления доступом. Сервис обнаружения ресурсов сам по себе должен быть защищенным ресурсом, требующим авторизации, прежде чем к нему можно получить доступ. Для доступа к сервису обнаружения ресурсов требуется решение об авторизации.

Существует некоторая информация о местоположении данных, которая нуждается в защите, так как может раскрыть чувствительную, с точки зрения защиты персональных данных, информацию (например, местоположение медицинской карты может раскрыть характер заболевания).

Примечание — В некоторых ситуациях ответ сервиса обнаружения ресурсов может быть единообразным для всех субъектов и неизменным в течение длительных периодов времени. Соответственно, ответ может осуществляться с помощью статических метаданных, а не динамически. Кроме того, в некоторых реализациях системы управления доступом сервис обнаружения ресурсов может также функционировать как сервис токенов безопасности, предоставляя субъекту токен доступа к ресурсам взамен токена, представленного субъектом для получения доступа к сервису обнаружения ресурсов.

5.3.2.5 Этапы получения доступа к ресурсам

Контролируемый доступ к ресурсам может быть осуществлен с использованием следующих этапов:

а) аутентифицированный субъект может начать доступ с сервиса начального обнаружения, где он выясняет местоположение точки принятия решений по политике и сервиса токенов безопасности;

б) субъект запрашивает у точки принятия решений по политике авторизацию для доступа к определенным ресурсам. На основе политики или набора политик, предоставленных точкой информирования по политике, точка принятия решений по политике определяет, следует ли предоставлять авторизацию;

в) если авторизация доступа предоставляется, то компонент сервиса токенов безопасности точки принятия решений по политике генерирует токен доступа и передает субъекту;

г) если от сервиса начального обнаружения не было получено местоположение ресурса, субъект получает эту информацию от сервиса обнаружения ресурсов. В это время сервис обнаружения ресурсов может принимать токен доступа субъекта и предоставлять взамен токен доступа, который субъект может использовать для доступа к ресурсам;

д) субъект представляет токен доступа точки соблюдения политики для получения доступа к ресурсу.

Примечание — Доступ к ресурсу может осуществляться двумя способами:

- прямым образом к точке соблюдения политики с получением субъектом доступа к отдельным ресурсам, используя токен доступа;

- непрямым образом через сервис взаимодействия вместо осуществления запроса точки соблюдения политики для каждого необходимого ему ресурса.

Примером последней ситуации является случай, когда субъект не хочет раскрывать свои идентификационные данные ресурсам.

5.3.3 Реализация, ориентированная на организацию

5.3.3.1 Обзор

На рисунке 7 приведена ситуация ориентированного на организацию управления доступом, где решающую роль играет точка соблюдения политики.

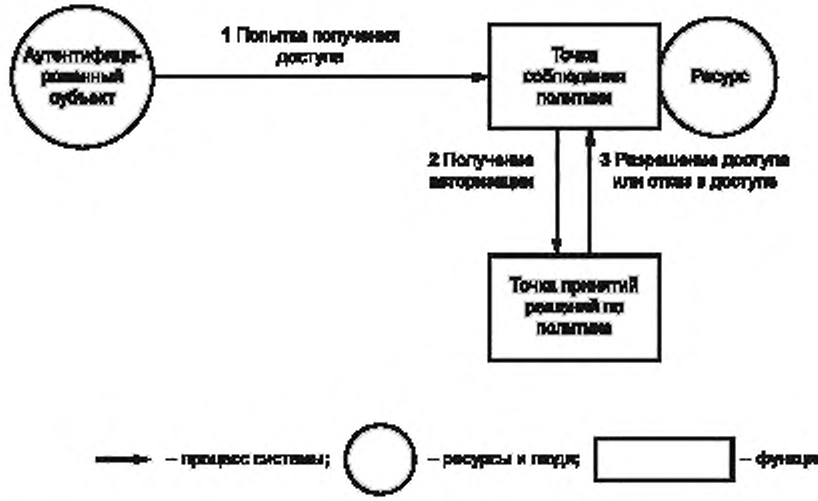

Рисунок 7 — Взаимодействие компонентных сервисов в реализации, ориентированной на организацию

5.3.3.2 Взаимодействие между точкой соблюдения политики и точкой принятия решений по политике

Реализация точки соблюдения политики и точки принятия решений по политике как независимых сервисов может обеспечить гибкость и эффективность при разработке систем управления доступом, особенно в ситуациях широкого распределения ресурсов.

Если политика разграничения доступа меняется, то, скорее всего, потребуется изменить только точку принятия решений по политике, а точка соблюдения политики будет продолжать функционировать без изменений.

Между точкой принятия решений по политике и точкой соблюдения политики должны существовать доверительные отношения.

Если точка соблюдения политики и точка принятия решений по политике не расположены вместе в защищенной сети, коммуникации между ними должны быть защищены. Точка соблюдения политики и точка принятия решений по политике должны быть способны аутентифицировать друг друга.

5.3.3.3 Этапы получения доступа к ресурсам

Контролируемый доступ к ресурсам может быть осуществлен с использованием следующих этапов:

а) аутентифицированные субъекты делают запрос о доступе к ресурсу точке соблюдения политики, передавая с запросом подтверждение идентификационных данных;

б) точка соблюдения политики направляет запрос доступа точке принятия решений по политике для получения авторизации, чтобы субъект получил доступ к ресурсу;

в) в точке принятия решений по политике принимается решение о доступе на основе привилегий доступа субъекта и политики доступа для ресурса. Она передает решение о доступе обратно точке соблюдения политики;

г) точка соблюдения политики обеспечивает выполнение решения о доступе.

6 Дополнительные требования и вопросы

6.1 Доступ к административной информации

Доступ к административным компонентам системы управления доступом должен быть ограничен уполномоченными лицами, такими как администраторы, специалисты по обеспечению безопасности и аудиторы.

У владельцев ресурсов должна быть возможность осуществления управления атрибутами доступа для ресурсов, за которые они отвечают. Доступ к административной информации осуществляется

через интерфейс к точке администрирования политики. Информация о субъектах и атрибутах для доступа субъектов к ресурсам хранится в точке информирования по политике.

При разработке политики управления доступом для административной информации системы управления доступом нужно определять следующее:

- критерии авторизации каждого административного доступа к информации;
- условия и механизмы доступа к информации;
- условия использования информации;
- какие операции доступа к информации нужно фиксировать и с какими подробностями;
- продолжительность хранения таких записей, как аудиторские записи, записи о предупреждениях, должна определяться политикой управления доступом;
- срок действия и условия наиболее приоритетной учетной записи администратора системы управления доступом.

6.2 Модели разграничения доступа и вопросы политики

6.2.1 Модели разграничения доступа

Существует ряд моделей разграничения доступа, которые подходят для использования в распределенной сетевой среде. Для управления своими ресурсами организация может выбрать следующие модели:

- модель разграничения доступа на основе идентификационных данных;
- модель разграничения доступа на основе ролей;
- модель разграничения доступа на основе атрибутов;
- модель разграничения доступа на основе возможностей;
- модель разграничения доступа на основе псевдонимов.

Выбор между этими моделями не обязательно является исключающим и может настраиваться в соответствии с различными группами субъектов.

Примечание — Описание моделей разграничения доступа содержится в приложении А.

6.2.2 Политики управления доступом

Политики системы управления доступом включают в себя политики разграничения доступа к ресурсам и политики управления и администрирования самой системы управления доступом. Необходимо установление политик для этих видов деятельности вместе с критериями обеспечения соответствия и средствами мониторинга и оценки соответствия.

Политика будет зависеть от выбранной модели разграничения доступа и подробностей реализации, в то время как установление политики и ее соответствие будут зависеть от общих соображений, которые могут охватывать следующее:

- соответствие политики разграничения доступа используемой модели разграничения доступа;
- определение и установка привилегий и атрибутов разграничения доступа для доступа субъектов и административных целей в соответствии с общей политикой разграничения доступа и разрешенными операциями с ресурсами;
- ограничение доступа к ресурсам необходимым минимумом для выполнения требуемой операции;
- требование наличия аутентифицированных идентификационных данных физических лиц и сущностей с определенным уровнем доверия до рассмотрения авторизации;
- определение авторизации физических лиц и сущностей для осуществления запрашиваемых операций доступа к ресурсам;
- предоставление доступа или отказ в доступе к ресурсам в соответствии с критериями авторизации и политикой доступа в ответ на запросы о доступе;
- обеспечение защиты персональных данных, используемых при осуществлении операций управления доступом;
- реализацию мониторинга и запись транзакций доступа с достаточным уровнем детализации, позволяющим осуществлять аудит транзакций доступа с целью демонстрации выполнения системных требований и других требований нормативных документов.

Политика может быть документально оформлена на неформальном (естественном) языке (см. 5.2.1). Впоследствии эта политика должна быть переведена в формальную политику. Нужно подтвердить, что формальная политика эквивалентна политике на естественном языке. Должны быть сформированы приемлемые доказательства соответствия этим требованиям.

6.3 Правовые и нормативные требования

Реализация системы управления доступом должна соответствовать любым правовым и нормативным требованиям, применимым в юрисдикциях ее использования. Например, могут существовать некоторые правовые и нормативные требования относительно:

- мониторинга и записи событий доступа;
- управления чувствительной, с точки зрения защиты персональных данных, информацией.

7 Практические приемы

7.1 Процессы

7.1.1 Процесс авторизации

В случаях, когда авторизация должна быть реализована как сервис, интерфейс сервиса может использовать существующие стандарты, например [6] и [7].

7.1.2 Процесс управления привилегиями

7.1.2.1 Обзор

Процесс управления привилегиями реализует политику разграничения доступа для области применения путем присвоения привилегий доступа к ресурсам.

Примечание — В случае использования модели разграничения доступа на основе ролей процесс управления привилегиями будет обеспечивать следующие функции:

- назначение людей на роли и установление закрепленных привилегий ролей;
- обеспечение уверенности в том, что эти лица подходят для выполнения роли и присвоения привилегий ролей;
- присвоение соответствующего атрибута названия роли лицам, которые будут действовать в этой роли;
- присвоение соответствующих привилегий разграничения доступа к ресурсам названию роли.

Если связанные с ролью привилегии должны быть изменены, следует провести проверку лиц, назначенных на эту роль, чтобы убедиться, что они по-прежнему подходят для выполнения этой роли с новыми привилегиями. Если это не выполнимо, следует отменить назначение соответствующих лиц на эту роль.

7.1.2.2 Доступность информации о привилегиях

Информация о привилегиях субъекта, необходимая для разграничения доступа к защищенным ресурсам, фиксируется в точке информирования по политике и предоставляется точке принятия решений по политике по запросу.

Примечание — Информация о привилегиях субъекта может включать в себя персональные данные и требовать защиты от несанкционированного раскрытия.

Политики разграничения доступа должны дополнительно включать в себя следующие меры:

- при необходимости получения субъектом доступа к ресурсу на основании доверительных отношений или доверенной третьей стороны ресурс должен сохранять свои обычные разрешения атрибутов разграничения доступа независимо от того, находится ли ресурс в организации исходного владельца ресурса или в организации запрашивающего субъекта. Ресурс должен иметь возможность авторизовать доступ или возвратиться к режиму доступа владельца ресурса для нового запроса авторизации, как будто данные все еще находятся в организации-владельце;
- меры, связанные с защитой информации организации, должны обеспечить защиту передачи данных между системами и действующими субъектами внутри организации-владельца ресурса и вовне к другим организациям, когда доступ к ресурсу осуществляется от доверенной третьей стороны. Такая защита не должна допускать, чтобы определенные данные покидали организацию в любом случае и особенно в случае сбоя при управлении доступом. Данная мера может включать в себя, например фильтры электронной почты.

7.2 Угрозы

Учитывая взаимодействие компонентных сервисов в реализации, ориентированной на организацию (рисунок 7), предполагается наличие следующих угроз во взаимодействии «запрос/ответ» между точкой соблюдения политики и точкой принятия решений по политике:

- имитация точки принятия решений по политике. Точка принятия решений по политике может быть поддельным сервисом;

- захват идентификатора субъекта. Нарушитель может использовать атаку перехвата сеанса связи в отношении идентификатора субъекта в токене доступа;

- изготовление идентификатора субъекта. Нарушитель может пытаться создать действительный идентификатор субъекта для токена доступа и использовать его, чтобы выдать себя за субъект;

- раскрытие информации токена доступа. Раскрытие токена доступа может сделать систему управления доступом уязвимой для других типов атак, поскольку он может содержать чувствительную информацию об авторизации и атрибутах;

- изготовление/модификация токена доступа. Нарушитель может создать поддельный токен доступа или изменить содержание токена доступа;

- подмена токена доступа. Субъект может пытаться выдать себя за субъект с более высокими привилегиями, нарушив канал связи между точкой принятия решений по политике и точкой соблюдения политики;

- повторное использование токена доступа. Нарушитель пытается использовать токен доступа, который уже использовался с предполагаемой точкой соблюдения политики;

- перенаправление токена доступа. Нарушитель использует токен доступа для одной точки соблюдения политики, чтобы получить несанкционированный доступ к другому ресурсу;

- угроза отказа в обслуживании. Случайная или намеренная угроза функционированию системы управления доступом, которая может привести к отказу в обслуживании субъектов.

Учитывая взаимодействие компонентных сервисов в реализации, ориентированной на субъекта (см. рисунок 6), предполагается наличие угроз не только в отношении коммуникаций между компонентными сервисами, но и в отношении используемого субъектом агента пользователя, поскольку через агента пользователя проходят чувствительные взаимодействия (коммуникации).

Следует рассмотреть меры противодействия, направленные на устранение этих угроз. Дополнительные рекомендации по определению соответствующих целей и средств управления содержатся в 7.3.

7.3 Цели управления

7.3.1 Общие положения

В данном подразделе излагаются цели управления, которые нужно верифицировать при планировании или пересмотре реализации системы управления доступом:

- рассматриваются задачи, которые должны быть решены до создания системы управления доступом;

- определяются цели внедрения системы управления доступом;

- определяются цели функционирования системы управления доступом.

Кроме того, общие цели и меры обеспечения информационной безопасности, изложенные в ГОСТ Р ИСО/МЭК 27002, также имеют отношение к системе управления доступом.

7.3.2 Валидация структуры управления доступом

7.3.2.1 Документальное оформление основ управления доступом

а) Цель

Целью является создание структуры управления для инициирования и внедрения управления доступом субъектов.

Должны быть документально оформлены группы субъектов, распознаваемых в структуре, процесс их аутентификации, политики разграничения доступа и утвержденные модели, идентифицированные точки соблюдения политики, средства, с помощью которых каждый распознаваемый субъект может быть проверен на протяжении всего своего жизненного цикла в системе и ему может быть предоставлена авторизация для доступа к ресурсам в структуре, а также возможные расширения структуры в рамках объединения.

б) Сфера применения и ограничения

Назначение

Набор атрибутов, используемых для аутентификации и представления доступа к ресурсам, должен быть четко определен и задокументирован в рамках управления доступом.

Рекомендации по реализации

Границы структуры управления доступом должны обозначать пределы, в рамках которых могут быть проверены субъекты.

Цель или правовая причина и связанные с этим обстоятельства среды, где могут существовать субъекты, определяют границы, в которых система управления доступом может осуществлять свой контроль над субъектами.

Дополнительная информация

Среда, в которой определяются субъекты, формируется по отношению к определенной совокупности атрибутов, к которым система управления доступом может применять меры и средства управления.

Сфера действия и границы структуры управления доступом должны рассматриваться с учетом [4].

в) Документальное оформление политик

Назначение

Следует разработать и периодически пересматривать политики для поддержки ИТ-стратегии управления доступом, как указано в [8]. Эти политики должны включать в себя назначение, методы управления, роли и обязанности, процесс исключений, подход к обеспечению соответствия и ссылки на процедуры, стандарты и рекомендации. Их актуальность должна регулярно подтверждаться и утверждаться.

Рекомендации по реализации

Политики структуры управления доступом могут варьироваться в зависимости от выбранной реализации, но при реализации структуры управления следует установить ряд общих политик и заявлений о соответствии, учитывая следующие политики:

- политику разграничения доступа, определяющую цели и ограничения, которые должны быть реализованы при применении разграничения доступом в границах структуры, и реализующую общие соображения, изложенные в 6.2.2;
- политику соответствия требованиям защиты персональных данных при осуществлении операций управления доступом (см. 7.3.2.2);
- мониторинг и прослеживание (фиксирование) действий политики доступа, обеспечивающие достаточный уровень детализации истории для проведения аудита транзакций доступа с целью демонстрации соблюдения системных и других требований соответствия.

Дополнительная информация

Система управления доступом может быть ориентированной на субъекта, сосредоточенной на одной точке принятия решений по политике или в организации и распределенной по нескольким точкам принятия решений по политике. Каждый аспект реализации приводит к различному документированию требований политик.

Политика может быть документально оформлена на неформальном (естественном) языке. Впоследствии эта политика должна быть переведена в формальную политику. Необходимо подтвердить, что формальная политика эквивалентна политике на естественном языке. Должны быть сформированы приемлемые доказательства соответствия этим требованиям.

г) Идентификация субъектов, получающих доступ к ресурсам в структуре

Назначение

Обеспечение уверенности в том, что сущности, осуществляющие управление доступом субъектов к ресурсам (например, точка принятия решений по политике и точка соблюдения политики), распознаются в рамках управления доступом.

Рекомендации по реализации

Сущности, которые могут делать доказуемые заявления о действительности и/или правильности субъектов для получения доступа к ресурсам в структуре (например, точка принятия решений по политике, точка соблюдения политики), должны быть признаны в рамках управления доступом.

Следует также идентифицировать сущности, одобряющие управленческие и регулятивные обязанности по сохранению информации о привилегиях (точка информирования по политике).

Дополнительная информация

Сущность может сочетать в себе функции точки принятия решений по политике, точки соблюдения политики и точки информирования по политике.

д) Идентификация органов структуры управления

Назначение

Информация об органах, составляющих структуру управления доступом, т. е. система управления доступом, система управления идентификационными данными, орган, связанный с атрибутами, сервис токенов безопасности, точка информирования по политике, точка принятия решений по политике, точ-

ка соблюдения политики, сервис обнаружения конечных точек ресурса, должна быть документально оформлена и опубликована. Эти сущности охватывают точку принятия решений по политике, точку соблюдения политики и точку информирования по политике.

Рекомендации по реализации

Документация точки принятия решений по политике, точки соблюдения политики и точки информирования по политике должна, по крайней мере, охватывать требования проверки прав доступа к информации, требования от пользователей прав доступа к информации и условия авторизации и использования прав доступа к информации.

7.3.2.2 Защита персональных данных субъектов в случаях, когда это требуется

Назначение

Защита персональных данных должна обеспечивать в любое время как часть целей, зафиксированных в структуре управления доступом, на уровне доверия, который необходим субъектам.

Рекомендации по реализации

Структура управления доступом должна устанавливать необходимые меры и средства управления, обеспечивающие при необходимости сохранение защиты персональных данных физических лиц, с которыми она взаимодействует.

В структуре управления идентификацией должна быть документально оформлена любая информация, относящаяся к специальным категориям персональных данных, которую она обрабатывает, обеспечивая соответствие требованиям, указанным в [2].

Дополнительная информация

Требования обращения с идентификационной информацией, относящейся к специальным категориям персональных данных, приведены в [2], ГОСТ Р 59407 и ГОСТ Р ИСО/МЭК 27002.

7.3.2.3 Поддержка определений структуры управления доступом

Назначение

Должен быть описан процесс, обеспечивающий уверенность в поддержании документации структуры.

Рекомендации по реализации

Компоненты структуры управления доступом могут со временем использовать различные структуры информации о привилегиях и полномочиях для поддержки своих взаимодействий с сущностями. Могут создаваться и прекращать свое действие домены, а также могут меняться условия их применимости (например, изменение модели).

Проверки структуры управления доступом должны включать в себя управление, политики, процессы, структуры данных, технологию и стандарты, обеспечивающие контроль жизненного цикла важнейших компонентов, начиная с первоначальной установки и заканчивая выводом из эксплуатации и заменой в структуре, отражая любые изменения в документации системы управления доступом.

7.3.3 Валидация системы управления доступом

7.3.3.1 Обзор

Система управления доступом реализует меры и средства контроля субъекта при доступе к ресурсам в рамках структуры управления доступом. Система управления доступом работает на основе политик, моделей, сферы действия и ограничений, определенных на уровне структуры управления доступом. Управление безопасностью информации в соответствии с ГОСТ Р ИСО/МЭК 27002 в рамках организации предполагает, что во всех системах должен быть контролируемый доступ под надзором системы управления идентификационными данными (определенной и задокументированной, как указано в [4]) и системы управления доступом. Соответственно, обеспечение выполнения этой цели в соответствии с ГОСТ Р ИСО/МЭК 27002 обязывает систему управления доступом соответствовать ряду целей управления. Эти цели управления включают в себя:

- составление списка компонентов и структуры для функционирования мер и средств управления доступом;
- определение и документальное оформление моделей разграничения доступа;
- определение привилегий и атрибутов в рамках конкретных моделей разграничения доступа;
- определение и документальное оформление процессов авторизации;
- аудит и снижение рисков, связанных с системой управления доступом.

7.3.3.2 Компоненты системы управления доступом

а) Цель

Целью является внедрение и документирование системы управления доступом к ресурсам.

б) Компоненты системы управления доступом

Назначение

Система управления доступом должна, как минимум, включать в себя следующие элементы:

- центральную систему управления, способную осуществлять сбор информации об управлении доступом из различных проверенных источников (домены происхождения атрибутов) и удалять эту информацию, когда условия хранения информации о привилегиях перестают существовать;
- репозиторий информации о привилегиях, относящихся к типам сущностей, распознаваемым в доменах соответствующей структуры, с различными наборами атрибутов, семантикой и синтаксисом, идентифицирующими привилегии и условия их использования;
- компонент хранения, архивирующий информацию о привилегиях, которые перестали существовать;
- репозиторий присвоения привилегий, возможно, в рамках репозитория информации о привилегиях, собирающий любые ссылки на присвоении привилегий любому субъекту, упоминаемому в структуре управления доступом;
- интерфейсы управления для предоставления доступа к необходимой информации о привилегиях;
- компонент определения точек принятия решений, соблюдения, информирования и администрирования;
- генератор уникальных ссылочных идентификаторов привилегий, которым присваиваются уникальные идентификаторы пользователей и сообщаются в репозитории информации о привилегиях.

Все эти компоненты должны быть документально оформлены надлежащим образом.

Рекомендации по реализации

Системы управления привилегиями могут различаться по компонентам в зависимости от модели, разработанной для их реализации. Однако система управления привилегиями должна оставаться независимой, поскольку она должна отвечать функциональным требованиям, являющимся особыми и в значительной степени отличающимися от типовой ИТ-системы.

в) Документальное оформление моделей доступа

Назначение

Описание прав доступа (привилегий) при доступе к ресурсам в структуре, правил, определяющих способ присвоения привилегий распознанным субъектам, процессов санкционирования присвоения привилегий субъектам, процессов обновления или аннулирования привилегий, а также метода проверки доступа к ресурсам должны быть документально оформлены.

Рекомендации по реализации

В структуре управления доступом у субъекта может быть несколько присвоенных привилегий на основе различных моделей. В сфере применения структуры у субъекта могут быть ресурсы, авторизованные на основе конкретной модели, а в другой сфере применения он может стать отличающимся субъектом, распознаваемым с другими привилегиями в этой сфере действия. Репозиторий структуры управления доступом должен быть способен собирать разные авторизации различных субъектов, которых он распознает в рамках разных моделей доступа. Атрибуты, описывающие субъект в сфере действия, представляют собой значения, с которыми репозиторий структуры может связывать различные санкционированные привилегии.

Каждая привилегия и связанные с ней описания должны быть документально оформлены в репозитории структуры с подробностями, требуемыми моделью для присвоения и контроля привилегии, санкционированной для субъекта.

г) Коммуникации между компонентами системы управления доступом

Назначение

Коммуникации между компонентами, составляющими структуру управления доступом, должны быть определены и задействованы.

Рекомендации по реализации

Коммуникации между органами и системами, составляющими структуру управления доступом, должны определяться в терминах условий, ситуаций и ожидаемых результатов. Эти коммуникации должны быть защищены от любой утечки информации к любой стороне за пределами упомянутых компонентов.

Процедура должна четко определять условия коммуникаций между компонентами.

Регулярные аудиты должны подтверждать, что безопасность коммуникаций обеспечивается.

7.3.3.3 Установление привилегий

а) Цель

Целью является определение, документальное оформление и доведение до сведения информации о привилегиях.

б) Представление привилегий

Назначение

Доступ к ресурсам должен определяться на основе определенных привилегий, устанавливаемых по усмотрению владельца информации и включаемых в методы, используемые для контроля их присвоения и предоставления при доступе к информации.

Рекомендации по реализации

Привилегии должны быть определены в каждой системе и приложении в границах структуры управления доступа. Привилегии — это представление необходимых разрешений, которые должны быть назначены и предоставлены пользователям до получения доступа к запрашиваемой информации. Они являются инструментами управления, связанными с назначением доступа субъекта к ресурсам по отношению к определенным атрибутам.

Представление привилегий должно учитывать чувствительность информации, к которой осуществляется доступ, и различные методы, используемые для контроля за их предоставлением субъекту при доступе к этой информации. В зависимости от чувствительности информации может требоваться разный уровень доверия к подтверждению субъекта. Требования по условиям доступа к информации должны учитываться при проверке привилегий субъектов.

Дополнительная информация

Дополнительная информация об управлении доступом к информации содержится в ГОСТ Р ИСО/МЭК 27002.

в) Указание информации о привилегиях

Назначение

При разграничении доступа к информации и ее обработке необходимо соблюдать руководящие указания, определяющие требования к фиксированному набору атрибутов, составляющих привилегии для доступа к ресурсам. Значения атрибутов должны учитывать чувствительность информации, определяемую владельцем информации, должны быть проверены точкой соблюдения политики и опубликованы.

Рекомендации по реализации

Руководящие указания должны разъяснять значения ряда параметров или условий, которые должны быть проверены, прежде чем привилегия может быть присвоена отдельному лицу.

Доступ к информации, ее распространение и предоставление должны санкционироваться только на основе принципов «необходимого наличия» и «необходимого знания» и основываться на классификации информации. Владельцы информационных активов должны определять соответствующую классификацию информации, которая будет разъяснять ограничения для конкретных привилегий и связанных с ними ролей пользователей, а также меры защиты, учитывающие соответственные риски безопасности информации.

г) Обеспечение доверия при накоплении информации для контроля привилегий

Назначение

Все обязанности по обеспечению безопасности информации, связанные со сбором и управлением информацией о привилегиях, должны быть определены и распределены. Накопленная информация о привилегиях должна соответствовать уровням доверия к идентичности пользователя.

Рекомендации по реализации

Уверенность в правильности разграничения доступа пользователей при использовании конкретной привилегии должна быть уточнена при формировании информации, необходимой для контроля привилегий. Как правило, определяются по меньшей мере два уровня требований к аутентификации: один уровень основан на идентификации пользователя, с которым связан пароль и который должен быть проверен с некоторой строгостью; второй уровень основан на двух факторах, сочетающих первый метод с другим элементом, например одноразовым паролем, заданным электронным токеном.

7.3.3.4 Управление системой управления доступом

а) Цель

Целью является обеспечение уверенности в том, что система управления доступом достигает намеченных целей.

б) Администрирование системы управления доступом

Назначение

Администрирование системы управления доступом должно ограничиваться лицами, занимающимися ее сопровождением, соответствующими органами и полагающимися сторонами.

Рекомендации по реализации

Система управления доступом должна иметь интерфейсы и процедуры, необходимые для надлежащего сопровождения информации о доступе в соответствии с правами, определенными и санкционированными соответствующими уполномоченными органами.

в) Аудит системы управления доступом

Назначение

Система управления доступом и другие компоненты, необходимые для формирования структуры управления доступом, должны подвергаться ежегодным регулярным оценкам или аудитам, позволяющим снижать риски, связанные с системой управления доступом.

Рекомендации по реализации

Аудит или оценка должны подтверждать, что система управления доступом функционирует в соответствии с ее документированными политиками и процедурами и соответствует правовым и иным требованиям (например, требованиям защиты персональных данных).

Оценки или аудиты должны:

- включать в себя отчеты, описывающие операции, выполняемые системой управления доступом, в частности в отношении выполнения операционных политик;
- включать в себя проверку безопасности коммуникаций между компонентами структуры;
- подтверждать, что система управления привилегиями сообщает об определенных операциях (например, о наличии уязвимостей), оценивать, соответствуют ли операции применяемым политикам (например, по результатам контроля конфиденциальности), и предупреждать о любых расхождениях;
- включать в себя подотчетность субъекта.

Цели и средства контроля для снижения рисков, приведенные в 7.2, должны разрабатываться с учетом компонентов, составляющих систему управления доступом.

7.3.4 Утверждение технической поддержки внедренной системы управления доступом

Вопрос поддержки структуры управления доступом приведен в 7.3.2.3. Система управления доступом включает в себя множество компонентов, требующих технической поддержки.

7.3.4.1 Поддержка авторизаций

а) Цель

Целью является:

- обеспечение уверенности в том, что структура управления доступом может сохранять достигнутую эффективность самоконтроля посредством поддержки компонентов и процедур;
- обеспечение уверенности в поддержке и защите информации о привилегиях в структуре управления доступом.

б) Поддержка процессов авторизации субъекта при доступе к ресурсу

Назначение

Формализованный процесс проверки соответствия требований, описываемых компонентами привилегий, назначенным привилегиям субъекта по доступу к ресурсу, должен быть документально оформлен.

Рекомендации по реализации

Процесс санкционирования назначения субъекту привилегий должен осуществляться с участием владельца информации, к которой предоставляется доступ, и уполномоченных представителей. Он должен обеспечивать уверенность в том, что элементы управления, предусмотренные в назначенных привилегиях, проверены до назначения и предоставления привилегий субъекту.

Процесс должен разделять вопросы необходимого владения от необходимого знания. Принцип необходимого владения должен подтверждать обоснованность запроса доступа. Принцип необходимого знания должен, кроме того, проверять правильность условий доступа к информации (например, гарантии разделения обязанностей, гарантии конфиденциальности). Условия формулируются владельцем информации и проверяющими сторонами.

Процесс должен быть формализованным и минимизировать число проверок до количества, определяемого чувствительностью информации, к которой получают доступ. Он должен учитывать проверки по уже выполненному доступу к информации и которые могут быть условными требованиями для предоставления прав доступа (например, субъекты уже прошли аутентификацию в сети организации).

Назначение прав доступа в распределенной сетевой среде должно осуществляться с учетом всех доступных типов соединений, с рассмотрением различных ролей и профилей, с обеспечением уверенности в формальной проверке пересмотра прав и разделением проверок запроса, авторизации и администрирования.

Деловые потребности и фактический статус занятости должны периодически проверяться с целью повторного подтверждения назначения привилегий и при необходимости их удаления (см. также 7.3.4.2).

Применение и управление идентификационными данными пользователей и аутентификационной информацией должны подвергаться мониторингу, фиксироваться и архивироваться.

Дополнительная информация

Дополнительная информация об управлении доступом к информации содержится в ГОСТ Р ИСО/МЭК 27002.

в) Проверка назначений привилегий

Назначение

Информация о назначенных привилегиях должны регулярно проверяться на предмет ее точности и необходимости.

Рекомендации по реализации

Содержание управления доступом должно включать в себя политики, процессы, данные, технологию и стандарты для обеспечения уверенности в том, что ключевые компонентов структуры в течение их жизненного цикла контролируются.

Все ключевые компоненты должны иметь свои предназначения. Ответственные специалисты, контролирующие процесс авторизации, могут меняться с течением времени, а также могут изменяться технологии. Информацию, определяющую привилегии, необходимо контролировать и соответственно регулярно пересматривать.

Системы могут меняться с течением времени, создаваться или прекращать свое функционирование, а также могут изменяться условия их применимости (например, изменение модели управления доступом).

Процесс, гарантирующий сохранность информации о привилегиях, заданных в структуре управления, должен быть документально оформлен.

Изменения в присвоении привилегий должны регистрироваться для проверки.

7.3.4.2 Управление доступом пользователей

а) Цель

Целью является обеспечение уверенности в том, что присвоенные права доступа отражают необходимые потребности бизнеса и не создают рисков.

б) Проверка назначений прав доступа пользователей.

Назначение

Владельцы информации должны периодически пересматривать привилегии пользователей и их обоснование, используя формализованный процесс.

Рекомендации по реализации

Привилегии должны периодически пересматриваться, а бизнес-потребности в правах доступа должны быть повторно подтверждены. Периодичность пересмотра должна быть разъяснена владельцем информации и включена в процедуру пересмотра. Периодичность пересмотра должна быть связана с чувствительностью информации, к которой получают доступ (см. также руководства по классификации информации). Пересмотры должны фиксироваться для проверки.

В случае перехода пользователя с одного места работы на другое в рамках организации, привилегии должны пересматриваться, удаляться или заново распределяться.

Изменения в присвоении привилегий должны регистрироваться для проверки.

7.3.4.3 Управление мониторингом и учетом

Назначение

Назначения прав доступа, авторизации, предоставленные доступы и учет действий субъекта должны фиксироваться для аудита. При управлении аудитом необходимо определять условия отслеживания и архивирования информации о запросах доступа с целью подтверждения того, что функционирование системы управления доступом соответствует политике разграничения доступа.

Рекомендации по реализации.

Аудиторские журналы назначения привилегий, разрешений и положений должны храниться для проверки и отслеживания истории. Условия ведения учета должны быть определены владельцем информации. Он должен учитывать чувствительность информации, к которой получают доступ.

Приложение А
(справочное)

Модели разграничения доступа, существующие в настоящее время

А.1 Общая информация

В приложении А представлены модели разграничения доступа, которые могут быть приняты в качестве основы политики разграничения доступа.

А.2 Модели разграничения доступа

А.2.1 Общие положения

Изначально решения по разграничению логического доступа основывались на идентификационных данных субъекта, делающего запрос о выполнении операции с ресурсом. Это относится к способу управление доступом на основе идентификационных данных, в котором доступ к ресурсу индивидуально предоставлялся локально идентифицированному субъекту. Позднее появился аналогичный способ, в котором доступ к ресурсу предоставлялся локально определенным ролям, участником которых являлся субъект.

В случае запроса субъектом доступа к ресурсу уверенности в качестве идентификационных данных, групп и ролей часто недостаточно для выражения различных возможностей комбинаций предоставления доступа. Альтернативой является формализованное удовлетворение или отклонение запросов субъекта на основе произвольных атрибутов субъекта и произвольных атрибутов ресурса, а также условий среды, которые могут быть глобально распознаны и более соответствовать принятой политике доступа.

А.2.2 Дискреционное разграничение доступа

В случае дискреционного разграничения доступа (Discretionary Access Control) каждый ресурс имеет владельца, и каждый владелец может определять операции, которые другие субъекты могут выполнять с этим ресурсом. Модель дискреционного разграничения доступа дает возможность субъекту, которому были присвоены привилегии доступа к ресурсу, по своему усмотрению делегировать привилегии другим субъектам или группам субъектов.

А.2.3 Мандатное разграничение доступа

Мандатное разграничение доступа (Mandatory Access Control) чаще всего используется в системах, где приоритетом является обеспечение конфиденциальности данных.

Первоначально мандатное разграничение доступа было моделью безопасности, ограничивающей возможность владельцев ресурсов разрешать или отказывать в выполнении операций с объектами, размещенными в файловой системе. Изначально проверки применялись только на отдельном средстве вычислительной техники операционной системой, включающей ядро безопасности.

Мандатное разграничение доступа реализуется путем присвоения классификационной метки каждому файловому ресурсу. Классификации включают в себя категорию информации и уровень конфиденциальности, например конфиденциальная, секретная или совершенно секретная. Каждому субъекту присваивается аналогичная классификация, называемая допуском.

В случае запроса субъекта на доступ к определенному ресурсу система будет проверять привилегии субъекта, чтобы определить, будет ли разрешен доступ, но также будет сравнивать допуск субъекта с классификацией ресурса.

Модель мандатного разграничения доступа построена на модели дискреционного разграничения доступа с двумя дополнительными правилами мандатного разграничения доступа.

Разграничительное свойство безопасности — владельцы индивидуальных ресурсов могут назначать меры защиты объектов, которые они контролируют, исходя из модели дискреционного управления доступом.

Простое свойство безопасности — субъект с данным уровнем безопасности не может читать ресурс с более высоким уровнем безопасности (без чтения).

*-свойство (читается как «звездочка»-свойство) — субъект с данным уровнем безопасности не должен записывать данные в какой-либо ресурс с более низким уровнем безопасности (без записи).

*-свойство может применяться только при использовании определенных терминалов и/или между системами, обе из которых способны применять *-свойство.

Данное свойство безопасности может быть применено в распределенной среде. Когда субъект попытается прочитать содержимое ресурса, система будет проверять привилегии субъекта с целью определения, можно ли разрешить доступ для чтения с использованием правил дискреционного управления доступом, но также будет сравнивать допуск субъекта с классификацией ресурса и таким образом применять правило Простого свойства безопасности.

Администрирование правил мандатного разграничение доступа осуществляют не владельцы ресурсов, а специалисты по обеспечению безопасности.

А.2.4 Разграничение доступа на основе идентификационных данных

Модель разграничения доступа на основе идентификационных данных (Identity-based Access Control) использует такие механизмы, как списки управления доступом, которые содержат идентификаторы субъектов вместе с операциями, разрешенными с данным ресурсом.

Используемые идентификаторы несут на себе некоторую семантику, связанную с идентификационными данными субъекта.

Очень часто один и тот же идентификатор используется для всех ресурсов. Такая ситуация дает возможность связывать операции, выполняемые одним и тем же субъектом на разных серверах или машинах.

Идентификатор может быть аутентифицированным идентификатором, полученным после успешного аутентификационного обмена, или может быть включен в токен доступа.

В модели разграничения доступа на основе идентификационных данных идентификационные данные субъектов авторизуются и добавляются в список управления доступом вместе с соответствующими привилегиями доступа субъекта к ресурсам, чтобы впоследствии разрешить доступ субъекта к ресурсам. Если идентификатор совпадает с идентификатором, содержащимся в списке управления доступом, субъекту предоставляется привилегия выполнить с ресурсом операции, упомянутые для этого субъекта в списке управления доступом.

Управление списком управления доступом необходимо до любого конкретного запроса доступа и приводит к добавлению идентификатора в список управления доступом вместе с конкретными операциями для ресурса.

А.2.5 Разграничение доступа на основе ролей

Модель разграничения доступа на основе ролей (Role-based Access Control) использует такие механизмы, как списки управления доступом, которые содержат роли субъектов вместе с операциями, разрешенными с данным ресурсом.

Используемые роли обычно несут на себе определенную семантику, но совместно используются несколькими субъектами.

Роль может быть включена в токен доступа (push-модель) или может быть получена из каталога после успешной аутентификации (pull-модель).

Когда роль совпадает с ролью, содержащейся в списке управления доступом, субъекту предоставляется привилегия выполнить с ресурсом операции, упомянутые для этой роли в списке управления доступом.

Управление списком управления доступом необходимо до любого конкретного запроса доступа и приводит к добавлению роли в список управления доступом вместе с конкретными операциями для ресурса.

Преимуществом введения ролей является отсутствие необходимости перечислять в списке управления доступом идентификаторы для каждого субъекта. Назначение ролей при разграничении доступа на основе ролей эффективно при использовании статических организационных позиций.

Роль может быть унаследована через иерархию ролей и обычно отражает привилегии, необходимые для выполнения определенных операций в организации. Данная роль может относиться к одному субъекту или к нескольким субъектам.

А.2.6 Разграничение доступа на основе атрибутов

Модель разграничения доступа на основе атрибутов (Attribute-based Access Control) использует такие механизмы, как списки управления доступом, которые содержат атрибуты субъектов вместе с операциями, разрешенными с данным ресурсом.

Атрибуты могут быть включены в токен доступа (push-модель) или получены из каталога после успешной аутентификации (pull-модель).

Когда атрибут совпадает с атрибутом, содержащимся в списке управления доступом, субъекту предоставляется привилегия выполнить с ресурсом операции, упомянутые для этого атрибута в списке управления доступом.

Управление списком управления доступом необходимо до любого конкретного запроса доступа и приводит к добавлению атрибута в список управления доступом вместе с конкретными операциями для ресурса.

А.2.7 Разграничение доступа на основе псевдонимов

Модель разграничения доступа на основе псевдонимов (Pseudonym-based Access Control) использует такие механизмы, как списки управления доступом, которые содержат псевдонимы субъектов вместе с операциями, разрешенными с данным ресурсом.

Используемые псевдонимы не несут на себе никакой семантики, связанной с идентификационными данными субъекта.

Часто для каждого отдельного сервера или сервиса используются разные псевдонимы. В этом случае невозможно связать операции, выполняемые одним и тем же субъектом на разных серверах или машинах.

Псевдоним может быть аутентифицированным псевдонимом, полученным после успешного аутентификационного обмена, или может быть включен в токен доступа.

Когда псевдоним совпадает с псевдонимом, содержащимся в списке управления доступом, субъекту предоставляется привилегия выполнить с ресурсом операции, упомянутые для этого субъекта в списке управления доступом.

Управление списком управления доступом необходимо до любого конкретного запроса доступа и приводит к добавлению псевдонима в список управления доступом вместе с конкретными операциями для ресурса.

А.2.8 Разграничение доступа на основе возможностей

Модель разграничения доступа на основе возможностей (Capabilities-based Access Control) использует возможности, назначенные субъекту по отношению к требованиям ресурса по доступу.

При разграничении доступа возможности обычно реализуются в токенах доступа, которые выдаются доверенным органом субъектам, которым разрешен доступ к соответствующим ресурсам. Токен доступа содержит информацию, позволяющую проверить токен и выдавшего его (например, с помощью цифровых сертификатов и подписи) и определить разрешения для доступа субъекта к ресурсам. Токен доступа может также содержать информацию, позволяющую аутентифицировать субъекта как истинного владельца токена. Выдача субъекту токена доступа (возможности) авторизует субъекта для доступа к соответствующим ресурсам с заданными разрешениями.

Токен доступа в данной модели использует билеты[1)] возможностей, которые содержат два основных компонента: (a) идентификатор ресурса и (b) операции, разрешенные с этим ресурсом.

Эти билеты выпускаются уполномоченным органом. Точка принятия решений по политике будет доверять не всем органам, а в случае органов, которым она доверяет, будет принимать только билеты, содержащие определенный набор операций.

Таким образом, точка принятия решений будет управляться матрицей, содержащей несколько строк, где в каждой строке находится:

- идентификатор признанного органа, который может выпускать свидетельства возможностей;
- операция, которая может быть включена в свидетельство возможностей для данного признанного органа.

Возможность может быть включена в токен доступа (push-модель) или может быть получена из каталога после успешной аутентификации (pull-модель).

Когда свидетельство возможностей совпадает с содержимым строки матрицы, субъекту предоставляется привилегия выполнять с ресурсом операции, упомянутые в матрице.

Управление матрицей доступа необходимо до любого конкретного запроса доступа и приводит к добавлению в матрицу идентификатора признанного органа, выпускающего свидетельства возможностей, вместе с конкретными операциями, которые могут быть включены в возможности для данного признанного органа.

Для выполнения требований аудита необходима способность идентифицировать субъекта, который был авторизован для выполнения операции с ресурсом. Это осуществляется по-разному в зависимости от того, используется ли push-модель или pull-модель.

В push-модели возможность включена в токен доступа, и присутствующая в токене некоторая другая информация позволяет косвенно идентифицировать субъекта (обычно только при сотрудничестве органа, выдавшего токен доступа).

В pull-модели субъект сначала аутентифицируется, а используемый во время аутентификационного обмена идентификатор включается в контрольный журнал.

Процесс выпуска токена может быть однократной операцией, т. е. после выдачи токена доступа субъект может использовать его для многих запросов доступа, пока/если токен доступа не будет аннулирован. Обычно так происходит при использовании физических токенов доступа (например, смарт-карты). В других ситуациях выпуск токена доступа может носить временный характер с ограниченным сроком использованием токена (например, на сеанс; на транзакцию).

При управлении доступом на основе возможностей орган, выпускающий токены доступа, исполняет роль точки принятия решений по политике в системе управления доступом, причем решение встроено в токен. Субъект, запрашивающий доступ к ресурсу, представляет токен доступа непосредственно точке соблюдения политики ресурса. Точка соблюдения политики подтверждает достоверность токена доступа и выпускающего его органа и проверяет встроенные разрешения на доступ к ресурсу перед предоставлением субъекту доступа к ресурсу.

[1)] Tickets.

Библиография

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

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

[3] ISO 10181-3:1996 Информационные технологии. Взаимодействие открытых систем. Основы безопасности для открытых систем. Часть 3. Основы разграничения доступа (Information technology — Open Systems Interconnection — Security frameworks for open systems — Part 3: Access control framework)

[4] ISO/IEC 24760-2:2015 Информационные технологии. Методы и средства обеспечения безопасности. Основы управления идентичностью. Часть 2. Базовая архитектура и требования (Information technology — Security techniques — A framework for identity management — Part 2: Reference architecture and requirements)

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

[6] Standard O.A.S.I.S. Расширяемый язык разметки контроля доступа (XACML) версии 3.0 [Xtensible Access Control Markup Language (XACML) Version 3.0] (January 2013)

[7] Kantara Initiative Профиль управляемого пользователем доступа OAuth 2.0 [User-Managed Access (UMA) Profile of OAuth 2.0]

[8] Information Systems Audit and Control Association Руководство по обеспечению ИТ-безопасности с использованием COBIT (The IT Assurance Guide Using COBIT)

УДК 006.34:004.056:004.056.5:004.056.53:006.354 ОКС 35.030

Ключевые слова: атрибут, идентификация, идентификационные данные, система управления доступом, модель разграничения доступа

Технический редактор *И.Е. Черепкова*
Корректор *Р.А. Ментова*
Компьютерная верстка *Е.А. Кондрашовой*

Сдано в набор 24.05.2021. Подписано в печать 01.06.2021. Формат 60×84⅛. Гарнитура Ариал.
Усл. печ. л. 4,18. Уч.-изд. л. 3,76

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

Создано в единичном исполнении во ФГУП «СТАНДАРТИНФОРМ»
для комплектования Федерального информационного фонда стандартов,
117418 Москва. Нахимовский пр-т. д. 31, к. 2.
www.gostinfo.ru info@gostinfo.ru