ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р ИСО 21091— 2017

ИНФОРМАТИЗАЦИЯ ЗДОРОВЬЯ

Службы каталога поставщиков и субъектов медицинской помощи и других сущностей

(ISO 21091:2013, IDT)

Издание официальное

Москва
Стандартинформ
2017

Предисловие

1 ПОДГОТОВЛЕН Федеральным государственным бюджетным учреждением «Центральный научно-исследовательский институт организации и информатизации здравоохранения» Министерства здравоохранения Российской Федерации (ЦНИИОИЗ Минздрава) и Обществом с ограниченной ответственностью «Корпоративные электронные системы» (ООО «Корпоративные электронные системы») на основе собственного перевода на русский язык англоязычной версии международного стандарта, указанного в пункте 4

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 468 «Информатизация здоровья» при ЦНИИОИЗ Минздрава — постоянным представителем ISO/TC 215

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 21 июня 2017 г. № 570-ст

4 Настоящий стандарт идентичен международному стандарту ИСО 21091:2013 «Информатизация здоровья. Службы каталога поставщиков и субъектов медицинской помощи и других сущностей» (ISO 21091:2013 «Health Informatics — Directory services for healthcare providers, subjects of care and other entities», IDT).

При применении настоящего стандарта рекомендуется использовать вместо ссылочных международных стандартов соответствующие им национальные стандарты, сведения о которых приведены в дополнительном приложении ДА

5 ВВЕДЕН ВПЕРВЫЕ

Правила применения настоящего стандарта установлены в статье 26 Федерального закона от 29 июня 2015 г. № 162-ФЗ «О стандартизации в Российской Федерации». Информация об изменениях к настоящему стандарту публикуется в ежегодном (по состоянию на 1 января текущего года) информационном указателе «Национальные стандарты», а официальный текст изменений и поправок — в ежемесячном информационном указателе «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ближайшем выпуске ежемесячного информационного указателя «Национальные стандарты». Соответствующая информация, уведомление и тексты размещаются также в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет (www.gost.ru)

Содержание

Введение

Службы каталога поставщиков и субъектов медицинской помощи и других сущностей, ориентированные на информационные системы здравоохранения, предназначены для удовлетворения требований информационной безопасности при информационном взаимодействии медицинских работников, возникающем в процессе выполнения ими клинических и административных функций. Раскрытие и передача полной конфиденциальной информации о состоянии здоровья в сфере здравоохранения требуют интенсивного шифрования этой информации и управления доступом к ней. При использовании инфраструктуры открытых ключей в сфере здравоохранения создаются регистры сертификатов, содержащих деловую и профессиональную информацию, необходимую для выполнения транзакций обмена данными. В нее обязательно включается идентификация отдельных ролей, выполняемых в сфере здравоохранения, которые могут быть назначены только соответствующими организациями здравоохранения. Поэтому функции регистрации и управления должны широко использоваться и являются потенциально распределенными между субъектами сферы здравоохранения. Служба каталога должна обеспечивать поддержку таких дополнительных требований к информационной безопасности в здравоохранении.

Использование каталога является все более популярным методом обеспечения возможностей однократной аутентификации. Эта цель достигается путем включения в каталог атрибутов идентификации и аутентификации медицинских работников и других сущностей.

С помощью каталога можно обмениваться дополнительными атрибутами, которые могут использоваться для авторизации доступа. Для решения этой задачи схема каталога расширяется таким образом, чтобы в нее входили информация кадровой службы организации здравоохранения, информация о специфичных контактах в сфере здравоохранения и идентификаторы, используемые в здравоохранении.

В настоящем стандарте изложены требования к каталогу, специфичные для сферы здравоохранения, и по мере необходимости определены стандартные спецификации включения этой информации в каталог, используемый в сфере здравоохранения.

Наряду с техническими мерами информационной безопасности, описанными в других стандартах ИСО, информационное взаимодействие в сфере здравоохранения требует надежной «цепочки доверия», обладающей необходимой учетностью. Для управления такой цепочкой доверия в инфраструктуре открытых ключей пользователи (доверяющие стороны) должны иметь возможность получения правильных текущих сертификатов и информации об их статусах с помощью средств безопасного управления каталогом.

Каталог, используемый в здравоохранении, должен поддерживать стандартные возможности клиентского поиска с помощью протокола LDAP (lightweight directory access protocol — облегченный протокол доступа к каталогам) и предоставлять сервис-ориентированную архитектуру SOA (service oriented architecture), обеспечивающую возможность доступа к каталогу из любой среды. Специфичные требования к реализации, критерии поиска и поддержка каталога не входят в область применения настоящего стандарта.

Хотя специфичные меры информационной безопасности и спецификации управления доступом также не входят в область применения настоящего стандарта, тем не менее в связи с чувствительностью данных о состоянии здоровья и персональных данных, при передаче которых могут использоваться службы каталога, необходимо описать существенные элементы управления, используемые на уровне ветви, классов объектов и атрибутов. Для обеспечения целостности информации, представленной в каталоге, предназначенном для здравоохранения, должны быть предоставлены соответствующие процессы и процедуры, а ответственность за содержание каталога должна быть точно прописана в политике и регламенте. Ожидается, что будет применен соответствующий контроль доступа, управляющий тем, кто может читать, записывать или изменять все элементы каталога, предназначенного для здравоохранения. Это может быть обеспечено с помощью присвоения отдельным лицам, включенным в каталог, роли HCOrganizationalRole и назначения этой роли соответствующих полномочий (например, чтение, изменение, удаление) в конфигурации управления каталогом.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ИНФОРМАТИЗАЦИЯ ЗДОРОВЬЯ

Службы каталога поставщиков и субъектов медицинской помощи и других сущностей

Health Informatics. Directory services for healthcare providers, subjects of care and other entities

Дата введения — 2019—07—01

1 Область применения

Настоящий стандарт содержит минимальные спецификации служб каталога, предназначенных для здравоохранения. Он может быть применен для облегчения реализации информационного взаимодействия организаций, приборов, серверов, прикладных компонентов, систем, технических участников и устройств.

В настоящем стандарте представлена общая информация о каталоге и службах, необходимых для обеспечения безопасного обмена медицинской информацией по сетям общего пользования, использующего такую информацию и такие службы. Каталог, предназначенный для использования в здравоохранении, описан в нем с точки зрения сообщества, нуждающегося в обеспечении межучрежденческого, межрегионального и межгосударственного обмена медицинской информацией. Хотя в настоящем стандарте описано несколько разных возможностей, конкретная служба не обязана все их обеспечивать.

В дополнение к обеспечению служб информационной безопасности, в том числе управления доступом и конфиденциальностью, настоящий стандарт предусматривает спецификации других аспектов информационного взаимодействия, например адреса и протоколы взаимодействующих сущностей.

В настоящем стандарте предусмотрена также поддержка служб каталога, предназначенных для обеспечения идентификации медицинских работников, учреждений здравоохранения и субъектов медицинской помощи.

2 Нормативные ссылки

В настоящем стандарте использована нормативная ссылка на следующий документ, необходимый для его применения (для датированной ссылки следует использовать только указанное издание, для недатированной ссылки следует использовать последнее издание указанного документа, включая все поправки):

ISO/HL7 27931:2009, Data Exchange Standards — Health Level Seven Version 2.5 — An application protocol for electronic data exchange in healthcare environments (Стандарты обмена данными. Health Level Seven Version 2.5. Прикладной протокол электронного обмена данными в организациях здравоохранения)

3 Термины и определения

В настоящем стандарте использованы следующие термины с соответствующими определениями:

3.1

контроль доступа (access control): Средства, с помощью которых ресурсы системы обработки данных предоставляются только авторизованным субъектам в соответствии с установленными правилами.

[ИСО/МЭК 2382-8]

Издание официальное

3.2

орган по присвоению атрибутов, OA (attribute authority; AA): Уполномоченный орган, назначающий полномочия путем выдачи сертификатов атрибутов.

[X.509]

3.3

сертификат атрибута (attribute certificate): Информационный объект, содержание которого заверено электронной подписью OA, привязывающий некоторые значения атрибута к идентификации его владельца.

[X.509]

3.4

аутентификация (authentication): Процесс надежной идентификации субъекта информационной безопасности путем защищенной ассоциации, установленной между идентификатором и субъектом.

[ИСО 7498-2]

3.5

авторизация (authorization): Процесс предоставления субъекту полномочий, в том числе предоставление доступа на основе полномочий доступа.

[ИСО 7498-2]

3.6

доступность (availability): Свойство находиться в состоянии готовности и возможности использования по запросу авторизованного логического объекта.

[ИСО 7498-2]

3.7 **сертификат** (certificate): Сертификат открытого ключа.

3.8 **распространение сертификатов** (certificate distribution): Акт издания сертификатов и их передачи принципалам безопасности.

3.9

издатель сертификата (certificate issuer): Уполномоченный орган, которому одна или несколько участвующих сторон доверили создание и присвоение сертификатов.

[ИСО/МЭК 9594-8]

Примечание — Издатель сертификата дополнительно может создавать ключи для доверяющих сторон.

3.10 **управление сертификатами** (certificate management): Процедуры, имеющие отношение к сертификатам: генерация сертификатов, распространение сертификатов, архивирование и отзыв сертификатов.

3.11 **отзыв сертификата** (certificate revocation): Акт аннулирования достоверной связи между сертификатом и его владельцем (или владельцем принципала безопасности) вследствие того, что сертификату больше нельзя доверять, хотя срок его действия и не истек.

3.12 **список отозванных сертификатов;** COC (certificate revocation list; CRL): Опубликованный список отозванных или приостановленных сертификатов (заверенный электронной подписью УЦ).

3.13 **проверка сертификата** (certificate verification): Проверка аутентичности сертификата (3.7).

3.14 **удостоверяющий центр;** УЦ (certification authority; CA). Уполномоченный орган, которому одна или несколько участвующих сторон доверили создание и присвоение сертификатов и который дополнительно может создавать ключи для доверяющих сторон.

Примечания

1 Заимствовано из ИСО/МЭК 9594-8:2008.

2 Слово «центр» в термине «удостоверяющий центр» означает всего лишь доверенную сторону, а не какое-либо государственное лицензирование.

3 Более удачным термином может быть «издатель сертификата», но термин «удостоверяющий центр» очень широко употребляется.

3.15

конфиденциальность (confidentiality): Свойство информации быть недоступной и закрытой для неавторизованного лица, логического объекта или процесса.

[ИСО 7498-2]

3.16

целостность данных (data integrity): Свойство данных не подвергаться несанкционированному изменению или уничтожению.
[ИСО 7498-2]

3.17

электронная подпись (digital signature): Данные, добавленные к блоку данных, или криптографическое преобразование этого блока, позволяющие получателю блока данных убедиться в подлинности источника и целостности блока и защитить его от искажения, например, получателем.
[ИСО 7498-2]

3.18

идентификация (identification): Выполнение проверок, позволяющих системе обработки данных распознавать объекты.
[ИСО/МЭК 2382-8]

3.19

идентификатор (identifier): Информационный объект, используемый для объявления идентичности перед тем, как получить подтверждение соответствия от определенного аутентификатора.
[ENV 13608-1]

3.20

целостность (integrity): Свойство данных не подвергаться несанкционированному изменению или уничтожению.
[ИСО 7498-2]

3.21

ключ (key): Последовательность символов, управляющая операциями зашифрования и расшифрования.
[ИСО 7498-2]

3.22

управление ключами (key management): Генерация, сохранение, распределение, удаление, архивирование и применение ключей в соответствии с политикой безопасности.
[ИСО 7498-2]

3.23 **облегченный протокол доступа к каталогам** (lightweight directory access protocol; LDAP): стандартный протокол доступа к каталогам, обеспечивающий публичный или контролируемый доступ к сертификатам и иной информации, необходимой инфраструктуре открытых ключей.

3.24 **объектный идентификатор,** ОИД (object identifier OID): Уникальный алфавитно-цифровой идентификатор, регистрируемый в соответствии со стандартом регистрации идентификаторов ИСО и предназначенный для ссылки на конкретный объект или класс объектов.

3.25

неприкосновенность личной жизни (privacy): Защита от вмешательства в частную жизнь или деловые отношения отдельного лица, результатом которого являются неоправданный или незаконный сбор и использование персональных данных этого лица.
[ИСО/МЭК 2382-8]

3.26

закрытый ключ (private key): Ключ, используемый в асимметричном криптографическом алгоритме, обладание которым ограничено (обычно принадлежит только одному субъекту).
[ИСО/МЭК 10181-1]

3.27

открытый ключ (public key): Ключ, используемый в асимметричном криптографическом алгоритме, который может быть сделан общедоступным.
[ИСО/МЭК 10181-1]

3.28

сертификат открытого ключа; СОК (public key certificate; PKC): Сертификат, обеспечивающий связь идентичности с открытым ключом.
[RFC 3280]

3.29 **инфраструктура открытых ключей;** ИОК (public key infrastructure, PKI): Инфраструктура, включающая в себя аппаратное и программное обеспечение, людей, процессы и политики, которая использует технологию электронной подписи для предоставления доверяющим сторонам проверяемой ассоциации, установленной между открытым компонентом пары асимметричных ключей и конкретным субъектом.

3.30

доверяющая сторона (relying party): Получатель сертификата, доверяющий этому сертификату или электронной подписи, проверенной с помощью этого сертификата.
[RFC 3647]

3.31 **роль** (role): Комплекс способностей и/или действий, связанный с выполнением работы.

3.32

безопасность (security): Состояние защищенности, при котором обеспечиваются доступность, конфиденциальность, целостность и учетность.
[ENV 13608-1]

3.33

политика безопасности (security policy): Утвержденный план или способ действий по обеспечению информационной безопасности.
[ИСО/МЭК 2382-8]

3.34

служба безопасности (security service): Служба, предоставляемая уровнем взаимодействия открытых систем и обеспечивающая адекватную защиту систем или передачи данных.
[ИСО 7498-2]

3.35 **субъект безопасности, принципал** (security subject): Активный субъект, обычно представляющий лицо, процесс или устройство и инициирующий передачу информации между объектами или изменение состояния системы.

Примечание — Технически субъект представлен парой процесс/домен.

3.36 **субъект (subject):** Сущность, открытый ключ которой заверен сертификатом.

3.37 **субъект медицинской помощи** (subject of care): лицо, получающее, получившее или ожидающее получения медицинской помощи.

3.38 **третья сторона** (third party): Сторона, выполняющая определенную функцию безопасности как часть протокола обмена данными, но не являющаяся ни создателем, ни получателем данных.

3.39 **доверенная третья сторона;** ДТС (trusted third party; TTP). Третья сторона, считающаяся доверенной в рамках протокола информационной безопасности.

Примечание — Этот термин используется во многих стандартах ИСО/МЭК и в других документах, которые в основном описывают службы УЦ. Однако это понятие шире и включает в себя такие службы, как штампы времени и, возможно, депонирование ключей.

4 Сокращения

CA — удостоверяющий центр;
CN — общее имя;
CRL — список отозванных сертификатов; СОС;
DAP — протокол доступа к каталогам;
DIT — дерево информации каталога;
DN — отличительное имя;
EDI — электронный обмен данными;
LDAP — облегченный протокол доступа к каталогам;
MPI — главный регистр пациентов;

PDA — персональный цифровой помощник;
PIDS — служба идентификации лиц;
PKC — сертификат открытого ключа;
PKI — инфраструктура открытых ключей;
RA — центр регистрации; ЦР;
RDN — относительное отличительное имя;
TTP — доверенная третья сторона; ДТС.

5 Контекст здравоохранения

5.1 Общие сведения

Для учета нужд здравоохранения стандартные службы каталога должны быть расширены.

Атрибуты, определенные в стандарте X.500, не полностью удовлетворяют требованиям, предъявляемым к управлению идентификацией медицинских работников, субъектов медицинской помощи, организаций и других сущностей, вовлеченных в обмен медицинской информацией и принятие решений по информационной безопасности. Растущее применение вычислительных сетей для обмена медицинской информацией и управления ею увеличивает потребности включения в каталоги, специфичные для здравоохранения, дополнительной информации и дополнительных служб информационной безопасности. С ростом числа медицинских информационных систем, функционирующих в сети Интернет и в интрасетях, увеличивается и потребность обмена медицинской информацией между несколькими субъектами, в том числе не аффилированными, использующими как автоматическую передачу, так и диалоговый ввод данных. Для таких распределенных информационных взаимодействий в сфере здравоохранения требуется стандарт передачи данных, каталогов медицинских работников и сведений о получателях медицинской помощи.

Для упрощения функций управления пользователями и расширения функциональных возможностей организации все больше полагаются на развитые инфраструктуры информационных технологий, использующие LDAP и аналогичные службы и обеспечивающие управление центральным каталогом пользователей различных систем, развернутых в организации, в том числе доступ к этому каталогу. Такие инфраструктуры включают в себя корпоративные и учрежденческие каталоги, описания систем и служб, а также описания партнерских каталогов. В отличие от корпоративных моделей при применении подобных инфраструктур в системе здравоохранения должны быть сделаны существенные расширения контекста схемы, позволяющие представлять регуляторную информацию, клинические полномочия, многократное аффилирование на уровне медицинского работника и на организационном уровне, не аффилированных членов сообщества организаций здравоохранения, получателей медицинской помощи и деловых партнеров.

Кроме того, каталоги все шире применяются для аутентификации пользователей. Создавая единый источник управления пользователями, организации здравоохранения могут улучшить идентификацию пользователей, аутентификацию и процесс удаления идентификационных сведений о пользователе после прекращения его участия в организации. Предоставление средств «однократного входа» позволяет повысить безопасность управления паролями.

Каталоги могут также быть расширены в целях передачи атрибутов пользователей компонентам инфраструктуры информационной безопасности, отвечающим за принятие решения об авторизации. Включение в состав атрибутов сведений, специфичных для здравоохранения (например, роль и специализация), позволяет улучшить процессы предоставления и прекращения полномочий, управление ролями и доступом. Будучи эффективным средством повышения информационной безопасности, наличие таких атрибутов в то же время усложняет каталог и предъявляет дополнительные требования к взаимодействию между каталогами.

Другой службой информационной безопасности, предоставляемой каталогом в сфере здравоохранения, является поддержка инфраструктуры открытых ключей (ИОК). Такая служба использует каталог для хранения открытых ключей и обеспечения доступа к ним, а также для предоставления такой поддержки ИОК, как хранение списка отозванных сертификатов (СОС) и обеспечение доступа к нему. Поддержка ИОК и расширенной службы информационной безопасности также усложняет каталог вследствие дополнительных требований по описанию серверов, прикладных компонентов программного обеспечения и устройств.

Настоящий стандарт предусматривает несколько типов реализации каталогов. Служба каталога не обязана предоставлять все эти возможности. Это позволяет взаимодействующему домену создать

каталог, наиболее подходящий для ведения информации о конкретных организациях здравоохранения, людях или устройствах. Для поддержки ведения расписаний, уведомлений, взаимодействия поставщиков медицинской помощи и многих других функций могут создаваться каталоги поставщиков. С помощью таких каталогов может обеспечиваться проверка полномочий, необходимая при передаче сведений о санкционировании действий и статусе полномочий. Каталоги услуг могут использоваться для выполнения запросов, предоставляемых публично или определенным поставщикам медицинской помощи, например, для поиска специалиста в заданном географическом регионе. Каталоги, обеспечивающие информационное взаимодействие с субъектами медицинской помощи, должны обладать средствами повышенной защиты доступа, поэтому они должны управляться отдельно от каталогов поставщиков. Подобные каталоги могут также использоваться службами социальной защиты. Здесь перечислены только некоторые примеры применения каталогов в сфере здравоохранения. Дополнительные варианты использования приведены в приложении А к настоящему стандарту.

5.2 Физические лица — участники сферы здравоохранения

Хотя в стандарте X.500 и предусмотрен ряд классов объектов, представляющих физические лица и служащих, в этих классах отсутствует ключевая информация, специфичная для здравоохранения и требуемая для поддержки отраслевых информационных взаимодействий и служб. В каталогах, применимых в сфере здравоохранения, должна быть представлена такая профессиональная информация, как полномочия, идентификаторы, присвоенные организациями здравоохранения, ролевая информация и контактные данные, специфичные для здравоохранения. В связи с многократной аффилированностью, обсуждаемой в следующем разделе, такие контактные данные сложнее типичных данных, используемых в других отраслях. К физическим лицам — участникам сферы здравоохранения относятся:

- сертифицированные медицинские работники,
- не сертифицированные медицинские работники,
- другие работники медицинских организаций и работники вспомогательных организаций,
- субъекты медицинской помощи.

В этот список включены субъекты медицинской помощи в целях поддержки таких потенциальных приложений, как персональные медицинские карты, порталы пациентов и другие подобные приложения, в которых требуются службы онлайновой идентификации и аутентификации большого числа пользователей. В таких приложениях требуется найти баланс между базовой информацией, предусмотренной в каталоге, идентификацией субъекта медицинской помощи и информацией о соответствии заданной политике, например о соответствии с разрешенными способами использования информации. Реализации каталогов, обеспечивающих такие возможности для субъектов медицинской помощи, должны управляться отдельно от каталогов поставщиков медицинской помощи.

5.3 Многократное аффилирование

Во многих системах здравоохранения лица-участники могут быть аффилированы с несколькими организациями. В каждой такой организации эти лица могут иметь разные функции. Многие медицинские работники имеют частную практику, но при этом им разрешается практиковать в одной или нескольких организациях здравоохранения. Аналогично службы поддержки могут предоставляться нескольким организациям здравоохранения. В пределах одной и той же организации лицо может иметь разные роли в зависимости от места оказания медицинской помощи или других факторов. Потребители медицинской помощи обычно обращаются ко многим медицинским работникам и организациям. Чтобы минимизировать противоречивость, вызванную дублированием управления информацией, схема каталога, предназначенная для здравоохранения и учитывающая многократное аффилирование, должна позволять ссылки на первичные источники информации.

Другой важный фактор состоит в том, что медицинские работники сами бывают получателями медицинской помощи, и их профессиональную идентификацию надо отличать от идентификации в качестве пациентов. С точки зрения подходящего использования важно, чтобы профессиональная идентификация медицинского персонала была отделена от их идентификации в качестве физических лиц, поскольку цели ее использования отличаются для разных ролей или разного контекста.

5.4 Организации здравоохранения

Хотя в стандарте X.500 и предусмотрен ряд классов объектов, описывающих организации, их атрибутов недостаточно для представления информации, специфичной для здравоохранения и необходимой для выполнения требований к каталогам, используемым в здравоохранении.

Информация, специфичная для здравоохранения, включает в себя:
- идентификаторы, присвоенные регуляторными органами;
- вид предоставляемой медицинской помощи;
- места оказания медицинской помощи;
- контактные данные, требуемые функциям управления ключевой информацией.

К организациям здравоохранения относятся:
- лицензируемые организации здравоохранения (например, больницы, аптеки, поликлиники, станции скорой помощи, сестринские организации, специализированные организации);
- плательщики, вспомогательные организации (например, поставщики, службы диктофонного ввода, службы кодирования информации, службы обработки счетов за оказанную медицинскую помощь);
- регуляторные органы или органы мониторинга (например, профессиональные объединения, органы контроля заболеваемости, органы регистрации лекарственных препаратов, органы санитарно-эпидемиологического контроля).

5.5 Аппаратное и программное обеспечение

В стандарте X.500 предусмотрены классы объектов, представляющие серверы и прикладные программы. Однако устройства и программное обеспечение, предназначенные для здравоохранения, должны сертифицироваться и регулярно контролироваться, поэтому для них должны быть указаны особые атрибуты, соответствующие требованиям, предъявляемым к каталогам, используемым в здравоохранении. Кроме того, персональные цифровые помощники (PDA) и другие устройства могут иметь специфичные ассоциации с другими сущностями, зарегистрированными в каталоге, предназначенном для здравоохранения. Сведения об устройствах и программном обеспечении, включаемые в каталог, ограничиваются идентифицирующей информацией и коммуникационными параметрами, а также ассоциациями с физическими лицами и организациями. Каталог может использоваться для идентификации актива, но не для управления активами.

5.6 Службы контроля безопасности в здравоохранении

В каталоге должны быть представлены сертифицирующие органы здравоохранения, органы по присвоению атрибутов и центры регистрации. Кроме того, в каталоге должна иметься возможность публикации информации, относящейся к управлению ключами. Для поддержки ролевого управления в здравоохранении каталог должен позволять представлять компоненты, специфичные для здравоохранения. К ним относятся представления выполняемых служебных обязанностей, контактная информация, специфичная для этих обязанностей, сведения о профессиональных сертификатах и сертификатах атрибутов, выданных лицу — участнику системы здравоохранения. Непосредственная поддержка функциональных ролей не предусматривается.

6 Система управления безопасностью каталогов

Информационным ресурсам здравоохранения требуется система усиленных политик управления информационной безопасностью, обеспечивающая целостность передаваемых данных и инфраструктуры аутентификации. Подобные усиленные практические принципы уже определены в международных стандартах. Хотя следующие стандарты не специфичны для каталогов, они могут быть рекомендованы для защиты инфраструктур каталогов:
- ИСО/МЭК 27000;
- ИСО/МЭК 27001;
- ИСО 27799;
- ИСО 27005;
- спецификация COBIT, разработанная организацией Information Systems Audit and Control Foundation.

7 Интероперабельность

7.1 Требования

Каталоги, предназначенные для здравоохранения, должны иметь возможность контактировать с каталогами различных деловых партнеров и/или взаимно обмениваться с ними информацией. Для этих целей используются такие методы, как связывание в цепочки, репликация, отправка данных, а также

формирование одностороннего или двустороннего доверия между каталогами. В зависимости от приложения или службы некоторые из этих методов будут чувствительными к несогласованности схем.

К моделям интероперабельности предъявляются следующие иерархические требования:

a) они должны быть способны физически разделить базу/сообщество клиентов здравоохранения на контролируемые компоненты, предоставляющие развитые службы;

b) они должны быть способны обеспечить репликацию и управление балансировкой нагрузки;

c) в целях обеспечения эффективной производительности поиска (например, в соотношении 80/20) они должны быть способны ограничивать дерево поиска до конкретной географической или логической области;

d) для облегчения управления контролем доступа, требуемого для защиты конфиденциальной информации, хранящейся в каталоге (например, сертификаты субъектов медицинской помощи не должны быть общедоступными), они должны быть способны организовать дерево информации каталога таким образом, чтобы разрешения доступа относились к точкам ветвления;

e) они должны быть способны организовать дерево информации каталога таким образом, чтобы можно было обеспечить распределенный доступ к региональной информации системы здравоохранения.

7.2 Пространство имен/структура дерева

Чтобы эти требования могли быть детализированы согласованным образом и при этом учитывались существующие юрисдикции регуляторных органов здравоохранения, должны быть доступны следующее высокоуровневое пространство имен и структура дерева.

7.2.1 Страна

Во всех случаях на вершине дерева должна быть указана страна профессиональной юрисдикции здравоохранения. Если организация действует в нескольких странах, то должно быть обеспечено представление, описывающее подчинение организации разным юрисдикциям регуляторных органов здравоохранения.

c — обязательный атрибут.

7.2.2 Регион

В тех странах, где юрисдикция органа управления здравоохранением ограничена отдельным регионом (например, штатом в США), должен использоваться узел региона.

l — не обязательный атрибут.

7.2.3 Организация

В узлах организации должны быть представлены регуляторные органы здравоохранения, контролирующие деятельность медицинских работников, информация о которых включена в каталог. Эти узлы могут также использоваться для указания профессиональных организаций медицинских работников и институтов, медицинских организаций, научно-исследовательских организаций.

o — обязательный атрибут (удостоверяющий центр, профессиональная медицинская организация).

7.2.4 Организационная единица

В тех юрисдикциях, где под узлом организации выделены ветви для органов, контролирующих отдельные профессии, узел организации должен быть дополнительно представлен организационными единицами. Например, во многих юрисдикциях провизоры, врачи, стоматологи могут управляться отдельными государственными органами или департаментами.

ou — не обязательный атрибут.

7.2.5 Структурные роли

На каждом уровне иерархии могут существовать стандартные структурные роли и местные структурные роли. Понятие структурной роли описано в разделе 9 настоящего стандарта.

7.2.6 Повторяющиеся экземпляры сведений о физических лицах

Конкретное физическое лицо может быть представлено в системе несколько раз, при этом ему могут быть присвоены разные идентификаторы в контексте профессиональных полномочий, в контексте с принадлежностью к нескольким организациям здравоохранения или в других подобных случаях, когда уместно несколько раз указать данное лицо. Такое разделение представлений информации о лице с несколькими идентификаторами, присвоенными органами здравоохранения, может быть обеспечено с помощью классов объектов и дерева информации каталога, но классы объектов сами по себе не гарантируют, что требуемое разделение достигнуто. Для решения этой задачи могут быть использованы структуры разных общих имен, присваиваемых экземплярам сведений о физических лицах, в которых присутствуют идентификаторы, присвоенные разными органами здравоохранения.

В сфере здравоохранения существует потребность создавать и контролировать информационные компоненты идентификации участника разными регуляторными органами. Эти органы идентифицируют участника, используя разную административную и контактную информацию. Например, в связи с такими ситуациями, как разные места жительства, контактная информация и базовая коммуникационная информация в каждом виде лицензии и в каждой юрисдикции могут содержать конфликтующие атрибуты. Поэтому в том же самом каталоге для каждой юрисдикции должны быть сохранены отдельные экземпляры сведений о физическом лице. Лицо может быть зарегистрировано в каталоге и как субъект медицинской помощи, и как поставщик медицинской помощи. Чтобы гарантировать правильное использование персональных данных, важно также разделить в каталоге личные и профессиональные данные лица. Это может войти в противоречие с концепцией, согласно которой в каталоге для данного физического лица должна существовать только одна запись, но зато позволяет иметь правильное представление идентификации лица в системе здравоохранения в тех случаях, когда ему присвоена разная идентификация разными органами здравоохранения. Например, врач может иметь разрешение практиковать в нескольких юрисдикциях и в каждой из них имеет другой идентификатор и, может быть, другой адрес. В то время как дерево информации каталога содержит представления сведений об всех физических лицах, организациях и устройствах, оно не требует, чтобы все эти сведения содержались в одном физическом или логическом информационном пространстве. При необходимости, например для оптимизации производительности службы или из архитектурных соображений, они могут быть разделены. Конкретный каталог, предназначенный для здравоохранения, может содержать представления сведений о всех, некоторых или не содержать никаких сведений о действующих лицах, и эти представления могут быть созданы, используя централизованный или децентрализованный подход.

В каждой конкретной юрисдикции сертифицированный медицинский работник должен иметь единственное представление. С помощью описанной ниже роли HCOrganizationalRole это представление может быть указано в различных организациях и организационных единицах. При этом используется атрибут RoleOccupant, содержащий отличительное имя (DN) этого работника. Используя эту конструкцию, можно извлечь контактную информацию, специфичную для данной организации.

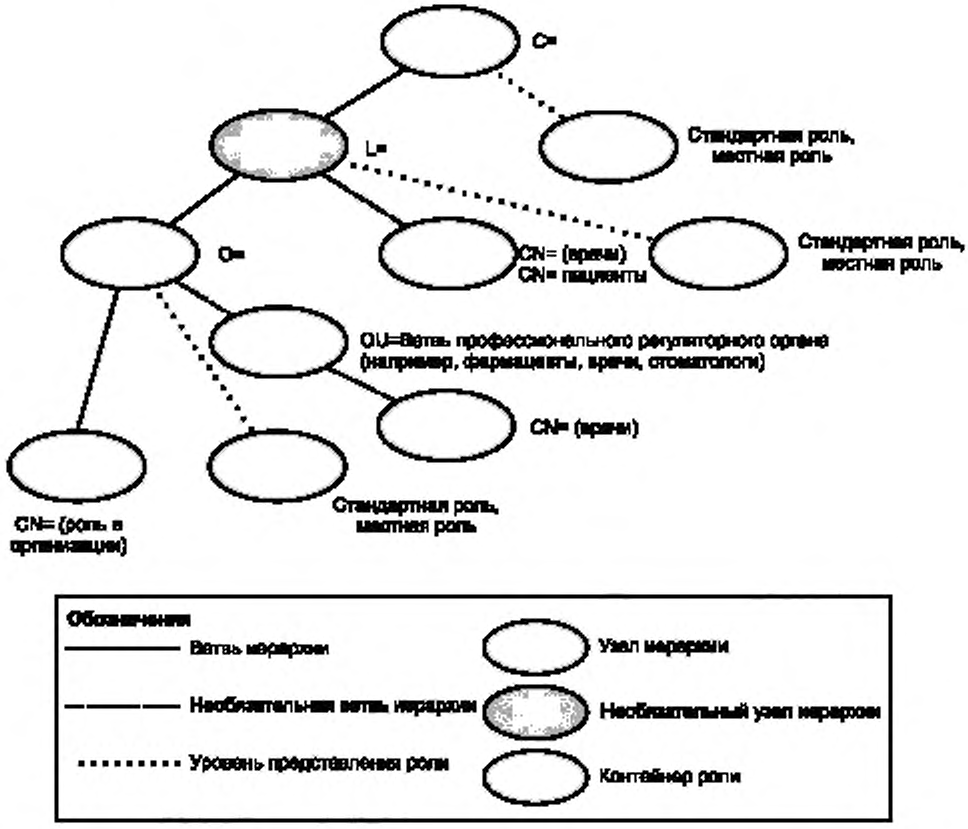

Рисунок 1 — Дерево информации каталога для здравоохранения

8 Схема каталога, предназначенного для здравоохранения

8.1 Физические лица — участники сферы здравоохранения

8.1.1 Общие сведения

В каталоге, предназначенном для здравоохранения, представлены многие типы физических лиц. Идентификация каждого лица должна быть представлена однократно, за исключением тех случаев, когда целесообразно иное. Примером такого исключения может быть представление идентификации медицинского работника, который сам стал пациентом. В этом случае она может быть представлена двумя объектами: один содержит профессиональную идентификацию, а второй — идентификацию, специфичную для субъекта медицинской помощи. Структура этих объектов должна быть специализациями родительского класса Person (физическое лицо). Такие специализации должны представлять следующие типы физических лиц: получатель медицинской помощи, медицинский работник, работник системы здравоохранения. Атрибуты классов объектов, специфичные для каждого из этих типов, должны добавляться как специализации базового класса. Тип «получатель медицинской помощи» выделен для целей идентификации, а не прямой поддержки процесса оказания медицинской помощи. В типе «медицинский работник» предусмотрены атрибуты, характеризующие признаки санкционирования, ограничения полномочий и другие подобные предупреждения.

Приведенные ниже схемы объектных классов включают в себя определения расширенных атрибутов по схеме, описанной в таблице 1.

Таблица 1 — Схема описания расширенных атрибутов

Атрибут	Имя нового поддерживаемого атрибута
ОИД	Объектный идентификатор, присвоенный новому атрибуту техническим комитетом ИСО/ТК 215
Описание	Описание нового атрибута
Синтаксис	Синтаксис, поддерживаемый протоколом LDAP и используемый для описания типа значения атрибута
Правила сравнения	Правила сравнения, используемые серверами при сопоставлении значений атрибута с заданным образцом в процессе выполнения операций поиска и сравнения
Кратный	Признак, обеспечивается ли возможность присваивания атрибуту нескольких значений

Спецификации расширения схемы указывают также, какие атрибуты обязательны, а какие — нет. Правила сравнения описаны в документе ITU-T X.520 (ИСО/МЭК 9594-6).

8.1.2 Субъекты (получатели) медицинской помощи

Класс объектов: HCSubjectOfCare

Родительский класс: Person

ОИД: 1.0.21091.1.1.1

Тип класса объектов: Структурный

Обязательные атрибуты класса HCSubjectOfCare описаны в таблице 2, необязательные — в таблице 3.

Таблица 2 — Обязательные атрибуты класса HCSubjectOfCare

Атрибут	ОИД	Описание	Синтаксис	Правила сравнения	Кратный
HcSubjectOfCareID	1.0.21091.2.1.29	Обезличенный, псевдонимизированный или опознаваемый идентификатор лица (Издатель:тип:ИД)	DirectoryString	caselgnoreMatch, caselgnoreSubstringsMatch	Да

С помощью конструкции (Издатель:тип:ИД) класс HcSubjectOfCareID может использоваться для представления любого типа идентификаторов, в том числе псевдонимизированный идентификатор, национальный идентификатор гражданина, номер полиса медицинского страхования, номер электронной медицинской карты и номер водительских прав. При этом в качестве альтернативы или дополнения может использоваться местная система кодирования.

Отдельные атрибуты из числа перечисленных в таблице 3 строго запрещены или ограничены некоторыми юрисдикциями. Поэтому важно, чтобы каждый атрибут каталога был проверен ответственным лицом или лицами на предмет, является ли он обязательным и юридически разрешенным. Необходимо также определить, каким пользователям и ролям разрешен доступ к каждому атрибуту.

Таблица 3 — Необязательные атрибуты класса HCSubjectOfCare

Атрибут	ОИД	Описание	Синтаксис	Правила сравнения	Кратный
HcIdentificationService	1.0.21091.2.0.2	Местонахождение услуги (услуг), предоставляющей идентификацию, например, службы перекрестной идентификации пациентов (PIX), служб электронной аутентификации, службы биометрической идентификации или другой службы проверки идентификации	DirectoryString	caseIgnoreMatch, caseIgnoreSubstringsMatch	Да
HcSigningCertificate	1.0.21091.2.0.3	Открытый ключ и сертификат, предназначенные для обеспечения неоспоримости подписи пользователя при информационном взаимодействии в здравоохранении	Binary	certificateExactMatch и certificateMatch	Да
HcAttributeCertificate	1.0.21091.2.0.4	Сертификат в формате P7, предназначенный для заверения полномочий, доверенности, принятых медицинских решений и т.д.	Binary	certificateExactMatch и certificateMatch	Да
HcMPILocation	1.0.21091.2.1.2	Местонахождение доступной службы (служб) главного регистра пациентов	DirectoryString	caseIgnoreMatch, caseIgnoreSubstringsMatch	Да
HcMedicalHome	1.0.21091.2.1.4	Местонахождение организации или частнопрактикующего врача, оказывающего комплексную медицинскую помощь	DirectoryString	caseIgnoreMatch, caseIgnoreSubstringsMatch	Нет
HcPHRLocation	1.0.21091.2.1.9	Местонахождение персональной медицинской карты субъекта медицинской помощи	DirectoryString	caseIgnoreMatch, caseIgnoreSubstringsMatch	Да
HcSubstituteDecisionMaker	1.0.21091.2.1.3	Идентификация записи о лице (лицах), способных подписывать документы или совершать иные действия по поручению субъекта	DN	distinguishedNameMatch	Да
HcMothersMaidenName	1.0.21091.2.1.30	Девичья фамилия матери субъекта медицинской помощи	DirectoryString	caseIgnoreMatch, caseIgnoreSubstringsMatch	Нет
HcDateTimeofBirth	1.0.21091.2.1.31	Дата и время рождения субъекта медицинской помощи	Дата в соответствии со стандартом ISO 8601	generalizedTimeMatch, generalizedTimeOrderingMatch	Нет

Продолжение таблицы 3

Атрибут	ОИД	Описание	Синтаксис	Правила сравнения	Кратный
HcSex	1.0.21091.2.1.32	Административный пол субъекта медицинской помощи. Допустимые значения определены в документе ISO/TS 22220	DirectoryString	caseIgnoreMatch, caseIgnoreSubstringsMatch	Нет
HcPatientAlias	1.0.21091.2.1.33	Псевдоним субъекта медицинской помощи.	DirectoryString	caseIgnoreMatch, caseIgnoreSubstringsMatch	Да
HcCountyCode	1.0.21091.2.1.34	Код региона места проживания субъекта медицинской помощи	DirectoryString	caseIgnoreMatch, caseIgnoreSubstringsMatch	Да
HcReligion	1.0.21091.2.1.35	Вероисповедание. Допустимые значения берутся из стандарта HL7. Примечание — в некоторых юрисдикциях использование этого атрибута строго запрещено	DirectoryString	caseIgnoreMatch, caseIgnoreSubstringsMatch	Да
HcBirthPlace	1.0.21091.2.1.36	Место рождения субъекта медицинской помощи	DirectoryString	caseIgnoreMatch, caseIgnoreSubstringsMatch	Нет
HcPatientDeathDateandTime	1.0.21091.2.1.37	Дата и время смерти субъекта медицинской помощи	Date	generalizedTimeMatch, generalizedTimeOrderingMatch	Нет
HcMultipleBirth	1.0.21091.2.1.38	Признак рождения субъекта медицинской помощи при кратных родах	DirectoryString	caseIgnoreMatch, caseIgnoreSubstringsMatch	Нет
HcMultipleBirthOrder	1.0.21091.2.1.39	Порядковый номер рождения субъекта медицинской помощи при кратных родах	DirectoryString	caseIgnoreMatch, caseIgnoreSubstringsMatch	Нет
preferredDeliveryMethod	2.5.4.28	RFC 2256: предпочтительный метод доставки	1.3.6.1.4.1.1466.115.121.1.14		Нет
St	2.5.4.8	Штат или провинция	DirectoryString	caseIgnoreMatch	Да
telexNumber	2.5.4.21	Номер телекса	TelexNumber		Да
L	2.5.4.7	Наименование региона	DirectoryString	caseIgnoreMatch	Да
postalCode	2.5.4.17	Почтовый индекс	DirectoryString	caseIgnoreMatch	Да
Street	2.5.4.9	RFC 2256: адрес улицы места проживания данного субъекта	DirectoryString	caseIgnoreMatch	Да
postalAddress	2.5.4.16	RFC 2256: почтовый адрес	PostalAddress	caseIgnoreListMatch	Да

Продолжение таблицы 3

Атрибут	ОИД	Описание	Синтаксис	Правила сравнения	Кратный
facsimileTelephoneNumber	2.5.4.23	RFC 2256: телефонный номер факсимильного устройства (факс)	FacsimileTelephoneNumber		Да
telephoneNumber	2.5.4.20	RFC 2256: телефонный номер	TelephoneNumber	telephoneNumberMatch	Да
teletexTerminalIdentifier	2.5.4.22	RFC 2256: идентификатор телексного терминала	1.3.6.1.4.1.1466.115.121.1.51		Да
postOfficeBox	2.5.4.18	RFC 2256: почтовый ящик	DirectoryString	caseIgnoreMatch	Да
destinationIndicator	2.5.4.27	RFC 2256: признак места назначения	PrintableString	caseIgnoreMatch	Да
userCertificate	2.5.4.36	RFC 2256: двоичный сертификат пользователя в соответствии со спецификацией X.509	Certificate		Да
uid	0.9.2342.19200300.100.1.1	RFC 1274: идентификатор пользователя	DirectoryString	caseIgnoreMatch	Да
homePostalAddress	0.9.2342.19200300.100.1.39	RFC 1274: почтовый адрес дома	PostalAddress	caseIgnoreListMatch	Да
preferredLanguage	2.16.840.1.113730.3.1.39	RFC 2798: письменный или устный язык общения, предпочтительный для данного лица	DirectoryString	caseIgnoreMatch	Нет
mail	0.9.2342.19200300.100.1.3	RFC 1274: почтовый ящик в формате RFC 822	IA5String	caseIgnoreIA5Match	Да
homePhone	0.9.2342.19200300.100.1.20	RFC 1274: номер домашнего телефона	TelephoneNumber	telephoneNumberMatch	Да
roomNumber	0.9.2342.19200300.100.1.6	RFC 1274: номер комнаты	DirectoryString	caseIgnoreMatch	Да
x500UniqueIdentifier	2.5.4.45	RFC 2256: уникальный идентификатор в каталоге X.500	BitString	bitStringMatch	Да
photo	0.9.2342.19200300.100.1.7	RFC 1274: фотография (факс G3)	1.3.6.1.4.1.1466.115.121.1.23		Да
businessCategory	2.5.4.15	RFC 2256: категория деловой активности	DirectoryString	caseIgnoreMatch	Да
pager	0.9.2342.19200300.100.1.42	RFC 1274: телефонный номер пейджера	TelephoneNumber	telephoneNumberMatch	Да
jpegPhoto	0.9.2342.19200300.100.1.60	RFC 2798: изображение в формате JPEG	JPEG		Да
audio	0.9.2342.19200300.100.1.55	RFC 1274: аудио (в формате u-law)	Audio		Да
userPKCS12	2.16.840.1.113730.3.1.216	RFC 2798: PKCS #12 личный идентификатор пользователя в соответствии с синтаксисом PFX PDU	Binary		Да

Окончание таблицы 3

Атрибут	ОИД	Описание	Синтаксис	Правила сравнения	Кратный
displayName	2.16.840.1.113730.3.1.241	RFC 2798: предпочтительное наименование при выводе содержания записей	DirectoryString	caseIgnoreMatch	Нет
mobile	0.9.2342.19200300.100.1.41	RFC 1274: номер мобильного телефона	TelephoneNumber	telephoneNumberMatch	Да
labeledURI	1.3.6.1.4.1.250.1.57	RFC2079: унифицированный идентификатор ресурса с дополнительным элементом	DirectoryString	caseExactMatch	Да
carLicense	2.16.840.1.113730.3. 1.1	RFC2798: лицензия или регистрационный номер транспортного средства	DirectoryString	caseIgnoreMatch	Да
givenName	2.5.4.42	RFC 2256: общий генерализованный тип имен лица	DirectoryString	caseIgnoreMatch	Да
userSMIMECertificate	2.16.840.1.113730.3.1.40	RFC2798: PKCS#7 подписанные данные, используемые для поддержки S/MIME	Binary		Да
initials	2.5.4.43	RFC 2256: общий генерализованный тип атрибутов имен лица	DirectoryString	caseIgnoreMatch	Да

Необязательное представление полей сегментов PID, использующее родительский класс и расширенные атрибуты

Вместо ряда полей, определенных в стандарте ISO/HL7 27931, Data Exchange Standards — Health Level Seven Version 2.5 (Health Level Seven Version 2.5. Прикладной протокол электронного обмена данными в организациях здравоохранения), должны использоваться атрибуты LDAP из числа описанных в таблице 2. При этом должно использоваться форматирование значений полей, предложенное в стандарте ISO/HL7 27931, с ограничениями, наложенными на атрибуты LDAP. Правила подстановки атрибутов LDAP приведены в таблице 4.

8.1.3 Медицинский работник

Класс объектов: HCProfessional

Родительский класс: InetOrgPerson

ОИД: 1.0.21091.1.1.2

Тип класса объектов: Структурный

Обязательные атрибуты описаны в таблице 5, необязательные — в таблице 6.

Таблица 4 — Правила подстановки атрибутов LDAP

Поле сегмента HL7 PID	Атрибут класса inetOrgPerson/HcSubjectOfCare
Фамилия, имя, отчество пациента	Фамилия, имя, отчество, форматированные в соответствии с типом данных XPN, включаются во второй экземпляр атрибута CN
Номер домашнего телефона	homePhone
Номер рабочего телефона	telephoneNumber
Основной язык пациента	preferredLanguage
Адрес пациента	homePostalAddress

Окончание таблицы 4

Поле сегмента HL7 PID	Атрибут класса inetOrgPerson/HcSubjectOfCare
Номер лицевого счета пациента	При необходимости используется атрибут HcSubjectOfCareID
Номер карточки социального страхования	При необходимости используется атрибут HcSubjectOfCareID
Номер водительских прав	При необходимости используется атрибут HcSubjectOfCareID

Таблица 5 — Обязательные атрибуты класса HCProfessional

Атрибут	ОИД	Описание	Синтаксис	Правила сравнения	Кратный
HcIdentifier	1.0.21091.2.0.1	Идентификатор в системе здравоохранения. Для сертифицированного медицинского работника должен как минимум содержать запись, указывающую идентификатор, присвоенный регуляторным органом (Издатель:тип:ИД:статус)	DirectoryString	caseIgnoreMatch, caseIgnoreSubstringsMatch	Да
HcProfession	1.0.21091.2.2.1	Текстовое представление профессии пользователя (Издатель: система кодирования: код)	DirectoryString	caseIgnoreMatch, caseIgnoreSubstringsMatch	Да
HcRegistrationStatus	1.0.21091.2.2.40	Признак, указывающий статус ограничений полномочий, наложенных регуляторным органом, или иное санкционирование деятельности	DirectoryString	caseIgnoreMatch, caseIgnoreSubstringsMatch	Да

Таблица 6 — Необязательные атрибуты класса HCProfessional

Атрибут	ОИД	Описание	Синтаксис	Правила сравнения	Кратный
HcIdentificationService	1.0.21091.2.0.2	Местонахождение службы или служб, предоставляющих услуги проверки биометрической или иной идентификации	DirectoryString	caseIgnoreMatch, caseIgnoreSubstringsMatch	Да
HcSigningCertificate	1.0.21091.2.0.3	Открытый ключ и сертификат, предназначенные для обеспечения неоспоримости подписи пользователя при информационном взаимодействии в здравоохранении	Binary	certificateExactMatch и certificateMatch	Да
HcAttributeCertificate	1.0.21091.2.0.4	Сертификат в формате P7, предназначенный для заверения полномочий, доверенности, принятых медицинских решений и т.д.	Binary	certificateExactMatch и certificateMatch	Да

Окончание таблицы 6

Атрибут	ОИД	Описание	Синтаксис	Правила сравнения	Кратный
HcRole	1.0.21091.2.0.5	(Издатель: система кодирования: код). Значением атрибута служит код роли из числа описанных в стандарте ИСО 21298. Могут использоваться другие коды роли, назначаемые организацией или регуляторным органом	DirectoryString	caselgnoreMatch, caselgnoreSubstringsMatch	Да
HcSpecialisation	1.0.21091.2.0.6	(Издатель: система кодирования: код). Значением атрибута служит код специальности из числа описанных в стандарте ИСО 21298. Могут использоваться другие коды специальности, назначаемые организацией или регуляторным органом	DirectoryString	caselgnoreMatch, caselgnoreSubstringsMatch	Да
HcPrincipalPractice Location	1.0.21091.2.2.3	Используется атрибут DN организации	DN	distinguishedNameMatch	Нет
HcPracticeLocation	1.0.21091.2.2.4	Используется атрибут DN организации	DN	distinguishedNameMatch	Да

8.1.4 Работники

Класс объектов: HCEmployee

Родительский класс: InetOrgPerson

ОИД: 1.0.21091.1.1.3

Тип класса объектов: Структурный

Обязательные атрибуты описаны в таблице 7, необязательные — в таблице 8.

Таблица 7 — Обязательные атрибуты класса HCEmployee

Атрибут	ОИД	Описание	Синтаксис	Правила сравнения	Кратный
HcIdentifier	1.0.21091.2.0.1	(Издатель:ИД). Идентификатор в системе здравоохранения. В качестве издателя может выступать работодатель	DirectoryString	caselgnoreMatch, caselgnoreSubstringsMatch	Да

Таблица 8 — Необязательные атрибуты класса HCEmployee

Атрибут	ОИД	Описание	Синтаксис	Правила сравнения	Кратный
HcIdentificationService	1.0.21091.2.0.2	Местонахождение службы или служб, предоставляющих услуги проверки биометрической или иной идентификации	DirectoryString	caselgnoreMatch, caselgnoreSubstringsMatch	Да

Окончание таблицы 8

Атрибут	ОИД	Описание	Синтаксис	Правила сравнения	Кратный
HcSigningCertificate	1.0.21091.2.0.3	Открытый ключ и сертификат, предназначенные для обеспечения неоспоримости подписи пользователя при информационном взаимодействии в здравоохранении	Binary	certificateExactMatch и certificateMatch	Да
HcAttributeCertificate	1.0.21091.2.0.4	Сертификат в формате P7, предназначенный для заверения полномочий, сертификатов, дипломов об образовании и т.д.	Binary	certificateExactMatch и certificateMatch	Да
HcRole	1.0.21091.2.0.5	(Издатель: система кодирования: код). Значением атрибута служит код роли из числа описанных в стандарте ИСО 21298. Могут использоваться другие коды роли, назначаемые организацией или регуляторным органом	DirectoryString	caseIgnoreMatch, caseIgnoreSubstringsMatch	Да
HcOrganization	1.0.21091.2.3.1	Используется для указания атрибута DN организации	DN	distinguishedNameMatch	Да

Для работника, не являющегося сертифицированным медицинским работником, в каталоге будет по одной записи для каждой организации здравоохранения, в которой он работает. Сертифицированные медицинские работники представлены с помощью класса HCOrganizationalRole, описанного в 9.2.5.2.

8.2 Идентификация организации

Организации должны быть представлены классом объектов, содержащим информацию, специфичную для организации. Эта информация должна включать в себя все атрибуты, требуемые для выполнения административных и медицинских функций. В каталоге должны быть представлены следующие типы организаций:

a) лицензируемые организации здравоохранения,

b) плательщики,

c) вспомогательные организации и регуляторные органы.

Для каждого типа организации должна быть предусмотрена своя специализация общего класса Organization, необходимая для выполнения требований, специфичных для системы здравоохранения. Например, в классе, описывающем плательщиков, может быть предусмотрен национальный идентификатор плательщика. Для работодателей может быть указан национальный идентификатор организации. Небольшие врачебные практики должны рассматриваться как лицензируемые организации здравоохранения, что позволяет включать в каталог необходимую часть не медицинского персонала этих практик. Регуляторные органы должны быть представлены как вспомогательные организации. Класс Organization описан в приложении B.

8.2.1 Лицензируемые организации здравоохранения

Класс объектов:	HCRegulatedOrganization
Родительский класс:	Organization
ОИД:	1.0.21091.1.1.4
Тип класса объектов:	Структурный

Обязательные атрибуты описаны в таблице 9, необязательные — в таблице 10.

Таблица 9 — Обязательные атрибуты класса HCRegulatedOrganization

Атрибут	ОИД	Описание	Синтаксис	Правила сравнения	Кратный
HcIdentifier	1.0.21091.2.0.1	(Издатель:ИД). Идентификатор в системе здравоохранения. В качестве издателя может выступать работодатель	DirectoryString	caseIgnoreMatch, caseIgnoreSubstringsMatch	Да

Таблица 10 — Необязательные атрибуты класса HCRegulatedOrganization

Атрибут	ОИД	Описание	Синтаксис	Правила сравнения	Кратный
HcSigningCertificate	1.0.21091.2.0.3	Открытый ключ и сертификат, предназначенные для обеспечения неоспоримости подписи пользователя при информационном взаимодействии в здравоохранении	Binary	certificateExactMatch и certificateMatch	Да
HcAttributeCertificate	1.0.21091.2.0.4	Сертификат в формате P7, предназначенный для заверения полномочий, сертификатов, дипломов об образовании и т.д.	Binary	certificateExactMatch и certificateMatch	Да
HcSpecialisation	1.0.21091.2.0.6	(Издатель: система кодирования: код). Значением атрибута служит код специальности из числа описанных в стандарте ИСО 21298. Могут использоваться другие коды специальности, назначаемые организацией или регуляторным органом	DirectoryString	caseIgnoreMatch, caseIgnoreSubstringsMatch	Да
EdiAdministrativeContact	1.0.21091.2.0.7	Информация о лице, ответственном за администрирование электронного информационного взаимодействия	DN	distinguishedNameMatch	Да
ClinicalInformationContact	1.0.21091.2.0.8	Информация о лице, ответственном за информирование по медицинским вопросам	DN	distinguishedNameMatch	Да
HcOrganizationCertificates	1.0.21091.2.0.9	Используется для хранения сертификатов организации здравоохранения	Binary	certificateExactMatch и certificateMatch	Да
HcClosureDate	1.0.21091.2.0.10	Дата закрытия организации или дата изменения ее наименования или подчиненности	Date	generalizedTimeMatch, generalizedTimeOrderingMatch	Нет
HcSuccessorName	1.0.21091.2.0.11	Атрибут DN записи организации-правопреемника	DN	distinguishedNameMatch	Да

Окончание таблицы 10

Атрибут	ОИД	Описание	Синтаксис	Правила сравнения	Кратный
HcRegisteredName	1.0.21091.2.4.1	Юридическое наименование организации, зарегистрированное регуляторным органом здравоохранения	DirectoryString	caseIgnoreMatch, caseIgnoreSubstringsMatch	Да
HcRegisteredAddr	1.0.21091.2.4.2	Адрес организации, зарегистрированный регуляторным органом. Он должен иметь ту же структуру, что и значение атрибута почтового адреса postalAddress	DirectoryString	caseIgnoreMatch, caseIgnoreSubstringsMatch	Да
HcServiceLocations	1.0.21091.2.4.3	Организации здравоохранения, оказывающие медицинскую помощь	DN	distinguishedNameMatch	Да
HcOperatingHours	1.0.21091.2.4.4	Рабочие часы организации	DirectoryString	caseIgnoreMatch, caseIgnoreSubstringsMatch	Да
HcSigningCertificate	1.0.21091.2.0.3	Открытый ключ и сертификат, предназначенные для обеспечения неоспоримости подписи пользователя при информационном взаимодействии в здравоохранении	Binary	certificateExactMatch и certificateMatch	Да

8.2.2 Организации-плательщики

Класс объектов: HCPayer

Родительский класс: Organization

ОИД: 1.0.21091.1.1.5

Тип класса объектов: Структурный

Обязательные атрибуты описаны в таблице 11, необязательные — в таблице 12.

Таблица 11 — Обязательные атрибуты класса HCPayer

Атрибут	ОИД	Описание	Синтаксис	Правила сравнения	Кратный
HcIdentifier	1.0.21091.2.0.1	(Издатель:ИД). Идентификатор в системе здравоохранения. В качестве издателя может выступать работодатель	DirectoryString	caseIgnoreMatch, caseIgnoreSubstringsMatch	Да

Таблица 12 — Необязательные атрибуты класса HCPayer

Атрибут	ОИД	Описание	Синтаксис	Правила сравнения	Кратный
HcSigningCertificate	1.0.21091.2.0.3	Открытый ключ и сертификат, предназначенные для обеспечения неоспоримости подписи пользователя при информационном взаимодействии в здравоохранении	Binary	certificateExactMatch и certificateMatch	Да

Окончание таблицы 12

Атрибут	ОИД	Описание	Синтаксис	Правила сравнения	Кратный
HcAttributeCertificate	1.0.21091.2.0.4	Сертификат в формате P7, предназначенный для заверения полномочий, сертификатов, дипломов об образовании и т.д.	Binary	certificateExactMatch и certificateMatch	Да
EdiAdministrativeContact	1.0.21091.2.0.7	Информация о лице, ответственном за администрирование электронного информационного взаимодействия	DN	distinguishedNameMatch	Да
ClinicalInformationContact	1.0.21091.2.0.8	Информация о лице, ответственном за информирование по медицинским вопросам	DN	distinguishedNameMatch	Да
HcOrganizationCertificates	1.0.21091.2.0.9	Используется для хранения сертификатов организации здравоохранения	Binary	certificateExactMatch и certificateMatch	Да
HcClosureDate	1.0.21091.2.0.10	Дата закрытия организации или дата изменения ее наименования или подчиненности	Date	generalizedTimeMatch, generalizedTimeOrderingMatch	Нет
HcSuccessorName	1.0.21091.2.0.11	Атрибут DN записи организации-правопреемника	DN	distinguishedNameMatch	Да
HcPayerProductID	1.0.21091.2.5.1	Наименование издателя: программа медицинской помощи: ИД	DirectoryString	caseIgnoreMatch, caseIgnoreSubstringsMatch	Да
HcOperatingHours	1.0.21091.2.4.4	Рабочие часы организации	DirectoryString	caseIgnoreMatch, caseIgnoreSubstringsMatch	Да

8.2.3 Вспомогательные организации (включая регуляторные органы)

Класс объектов:	HCSupportingOrganization
Родительский класс:	Organization
ОИД:	1.0.21091.1.1.6
Тип класса объектов:	Структурный

Обязательные атрибуты описаны в таблице 13, необязательные — в таблице 14.

Таблица 13 — Обязательные атрибуты класса HCSupportingOrganization

Атрибут	ОИД	Описание	Синтаксис	Правила сравнения	Кратный
HcIdentifier	1.0.21091.2.0.1	(Издатель:ИД). Идентификатор в системе здравоохранения. В качестве издателя может выступать работодатель	DirectoryString	caseIgnoreMatch, caseIgnoreSubstringsMatch	Да

Таблица 14 — Необязательные атрибуты класса HCSupportingOrganization

Атрибут	ОИД	Описание	Синтаксис	Правила сравнения	Кратный
HcSigningCertificate	1.0.21091.2.0.3	Открытый ключ и сертификат, предназначенные для обеспечения неоспоримости подписи пользователя при информационном взаимодействии в здравоохранении	Binary	certificateExactMatch и certificateMatch	Да
HcAttributeCertificate	1.0.21091.2.0.4	Сертификат в формате P7, предназначенный для заверения полномочий, сертификатов, дипломов об образовании и т.д.	Binary	certificateExactMatch и certificateMatch	Да
EdiAdministrativeContact	1.0.21091.2.0.7	Информация о лице, ответственном за администрирование электронного информационного взаимодействия	DN	distinguishedNameMatch	Да
ClinicalInformationContact	1.0.21091.2.0.8	Информация о лице, ответственном за информирование по медицинским вопросам	DN	distinguishedNameMatch	Да
HcOrganizationCertificates	1.0.21091.2.0.9	Используется для хранения сертификатов организации здравоохранения	Binary	certificateExactMatch и certificateMatch	Да
HcClosureDate	1.0.21091.2.0.10	Дата закрытия организации или дата изменения ее наименования или подчиненности	Date	generalizedTimeMatch, generalizedTimeOrderingMatch	Нет
HcSuccessorName	1.0.21091.2.0.11	Атрибут DN записи организации-правопреемника	DN	distinguishedNameMatch	Да
HcOperatingHours	1.0.21091.2.4.4	Рабочие часы организации	DirectoryString	caseIgnoreMatch, caseIgnoreSubstringsMatch	Да

8.3 Роли, служебная обязанность и группа

8.3.1 Роль лица в организации

Этой ролью является обязанность отдельного физического лица — работника или подрядчика, назначенная ему организацией. Лицо может иметь в организации одну или несколько обязанностей. Например, врач может выполнять в больнице и медицинские, и административные обязанности. Для каждой из них может быть указана своя контактная информация. В этом примере медицинская информация может направляться в одно место, а административная — в другое. Чтобы указать, что одно и то же лицо имеет несколько служебных обязанностей в одной или нескольких организациях, схема каталога должна содержать класс, не имеющий идентификатора пользователя (uid) и содержащий атрибут RoleOccupant типа DN. Учтите, что этот класс отличается от класса роли Role и назван ролью, чтобы обеспечить преемственность по отношению к классу, представляющему понятие роли, а именно, OrganizationalRole. Классы OrganizationalRole и GroupOfNames описаны в приложении Б.

Класс объектов:	HCOrganizationalRole
Родительский класс:	OrganizationalRole
ОИД:	1.0.21091.1.1.7

Тип класса объектов: Структурный

Дополнительные обязательные атрибуты отсутствуют. Необязательные атрибуты описаны в таблице 15.

Таблица 15 — Необязательные атрибуты класса HCOrganizationalRole

Атрибут	ОИД	Описание	Синтаксис	Правила сравнения	Кратный
HcAttributeCertificate	1.0.21091.2.0.4	Сертификат в формате P7, предназначенный для заверения полномочий, сертификатов, дипломов об образовании и т.д.	Binary	certificateExactMatch и certificateMatch	Да
HcRole	1.0.21091.2.0.5	(Издатель: система кодирования: код). Значением атрибута служит код специфичной служебной роли из числа описанных в стандарте ИСО 21298. Могут использоваться другие коды роли, назначаемые организацией или регуляторным органом	DirectoryString	caseIgnoreMatch, caseIgnoreSubstringsMatch	Да
mail	0.9.2342.19200300.100.1.3	Адрес электронной почты, предназначенной для коммуникации при выполнении данной роли	IA5String	caseIgnoreIA5Match или caseExactIA5Match	Да
HcResponsibleParty	1.0.21091.2.7.1	Атрибут DN лица или роли HCOrganizationalRole, ответственной за выполнение данной обязанности (медицинский персонал, юридический контроль, работа по контракту, служащий)	DN	distinguishedNameMatch	Да

8.3.2 Стандартная роль в здравоохранении

Класс Role является специальным типом класса Group, предназначенного для представления многих типов ролей в сфере здравоохранения. Эти типы должны быть ограничены стандартными ролями. Исполнители этих ролей должны идентифицироваться атрибутом DN организационной роли лица HCOrganizationalRole. Сами эти роли будут использоваться в качестве основы определения контроля доступа приложениями, запрашивающими у служб каталога аутентификацию на базе сертификатов SSL. Эти роли будут запрашиваться также медицинскими прикладными программами, которые могут ограничивать выполнение некоторых функций в зависимости от роли пользователя.

Класс объектов:	HCStandardRole
Родительский класс:	GroupOfNames
ОИД:	1.0.21091.1.1.8
Тип класса объектов:	Структурный

Дополнительные обязательные атрибуты отсутствуют. Необязательные атрибуты описаны в таблице 16.

Таблица 16 — Необязательные атрибуты класса HCStandardRole

Атрибут	ОИД	Описание	Синтаксис	Правила сравнения	Кратный
HcRole	1.0.21091.2.0.5	(Издатель: система кодирования: код). Значением атрибута служит код специфичной служебной роли из числа описанных в стандарте ИСО 21298. Могут использоваться другие коды роли, назначаемые организацией или регуляторным органом	DirectoryString	caseIgnoreMatch, caseIgnoreSubstringsMatch	Да
HcRoleValidTime	1.0.21091.2.0.12	Время в формате GMT, в течение которого пользователь может действовать в данной роли	DirectoryString	caseIgnoreMatch, caseIgnoreSubstringsMatch	Да
HcRoleLocationRestriction	1.0.21091.2.0.13	Ограничения местонахождения, допустимого для данной роли (например, только отделение скорой помощи, IP-адрес и т.д.)	DirectoryString	caseIgnoreMatch, caseIgnoreSubstringsMatch	Да

8.3.3 Местные роли

Организация назначают местные роли сервисным группам, не определенным в стандартах. Большинство требований контроля доступа должны формулироваться в терминах стандартных ролей. Если же требуются иные ограничения доступа, то должны быть выделены группы, удовлетворяющие таким специальным ограничениям.

Класс объектов: HCLocalRole

Родительский класс: GroupOfNames

ОИД: 1.0.21091.1.1.9

Тип класса объектов: Структурный

Дополнительные обязательные атрибуты отсутствуют. Необязательные атрибуты описаны в таблице 17.

Таблица 17 — Необязательные атрибуты класса HCLocalRole

Атрибут	ОИД	Описание	Синтаксис	Правила сравнения	Кратный
HcRole	1.0.21091.2.0.5	(Издатель: система кодирования: код). Значением атрибута служит код специфичной служебной роли из числа описанных в стандарте ИСО 21298. Могут использоваться другие коды роли, назначаемые организацией или регуляторным органом	DirectoryString	caseIgnoreMatch, caseIgnoreSubstringsMatch	Да
HcRoleValidTime	1.0.21091.2.0.12	Время в формате GMT, в течение которого пользователь может действовать в данной роли	DirectoryString	caseIgnoreMatch, caseIgnoreSubstringsMatch	Да

Окончание таблицы 17

Атрибут	ОИД	Описание	Синтаксис	Правила сравнения	Кратный
HcRoleLocationRestriction	1.0.21091.2.0.13	Ограничения местонахождения, допустимого для данной роли (например, только отделение скорой помощи, IP-адрес и т.д.)	DirectoryString	caseIgnoreMatch, caseIgnoreSubstringsMatch	Да

8.3.4 Кодированные справочные данные

В здравоохранении используется множество кодированных справочных данных. С помощью технологии каталога можно упростить доставку этих данных прикладным программам, управляющим информацией здравоохранения. При этом кодированная справочная информация хранится в атрибуте HcReferenceDescription как сочетание кода и его описания. Описанные ниже атрибуты образуют новый класс объектов, специфичный для здравоохранения.

Класс объектов: HCCodedReference

Родительский класс: Top

ОИД: 1.0.21091.1.1.10

Тип класса объектов: Вспомогательный

Обязательные атрибуты описаны в таблице 18, необязательные — в таблице 19.

Таблица 18 — Обязательные атрибуты класса HCCodedReference

Атрибут	ОИД	Описание	Синтаксис	Правила сравнения	Кратный
HcIssuingAuthority	1.0.21091.2.10.1	Орган, ответственный за схему кодирования	DirectoryString	caseIgnoreMatch, caseIgnoreSubstringsMatch	Да
HcReferenceEffectiveDate	1.0.21091.2.10.2	Дата, до которой действителен или был действителен справочный словарь	Date	generalizedTimeMatch, generalizedTimeOrderingMatch	Нет
HcReferenceDescription	1.0.21091.2.10.3	Сочетание «справочный код:описание»	DirectoryString	caseIgnoreMatch, caseIgnoreSubstringsMatch	Да

Таблица 19 — Необязательные атрибуты класса HCCodedReference

Атрибут	ОИД	Описание	Синтаксис	Правила сравнения	Кратный
HcVocabularyOID	1.0.21091.2.10.4	ОИД используемого словаря здравоохранения	ObjectIdentifier	objectIdentifierMatch	Нет
HcReferenceDateOfIssue	1.0.21091.2.10.5	Дата издания справочного словаря	Date	generalizedTimeMatch, generalizedTimeOrderingMatch	Нет
HcReferenceInvalidDate	1.0.21091.2.10.6	Дата, на которую справочный словарь прекратит или прекратил действие	Date	generalizedTimeMatch, generalizedTimeOrderingMatch	Нет
HcReferenceVersion	1.0.21091.2.10.7	Версия справочного словаря	DirectoryString	caseIgnoreMatch, caseIgnoreSubstringsMatch	Да

8.3.5 Устройства

Сведения об устройствах, хранимые в каталоге, должны соответствовать документу DICOM Supplement 67: Configuration Management или релевантным спецификациям устройств в стандартах ИСО, дополненными описанными ниже атрибутами.

Класс объектов: HCDevice

Родительский класс: Top

ОИД: 1.0.21091.1.1.11

Тип класса объектов: Вспомогательный

Дополнительные обязательные атрибуты отсутствуют. Необязательные атрибуты описаны в таблице 20.

Таблица 20 — Необязательные атрибуты класса HCDevice

Атрибут	ОИД	Описание	Синтаксис	Правила сравнения	Кратный
HcDeviceIssuedTo	1.0.21091.2.11.1	Значение атрибута DN лица, которому выдано устройство	DN	distinguishedNameMatch	Нет
HcDeviceDateOfIssue	1.0.21091.2.11.2	Дата выдачи устройства получателю	Date	generalizedTimeMatch, generalizedTimeOrderingMatch	Нет
HcDevicDateRecalled	1.0.21091.2.11.3	Дата отзыва устройства	Date	generalizedTimeMatch, generalizedTimeOrderingMatch	Нет
HcDeviceDateRetrieved	1.0.21091.2.11.4	Дата возвращения устройства	Date	generalizedTimeMatch, generalizedTimeOrderingMatch	Нет
HcDeviceCertificate	1.0.21091.2.11.5	Сертификат, выпущенный для устройства	Binary	certificateExactMatch и certificateMatch	Да
HcDeviceTrackingNumber	1.0.21091.2.11.6	(Издатель:номер). Инвентарный номер устройства	DirectoryString	caseIgnoreMatch, caseIgnoreSubstringsMatch	Да
HcDevicePhone	1.0.21091.2.11.7	Телефонный номер устройства (например, персонального цифрового помощника)	TelephoneNumber	telephoneNumberMatch и telephoneNumberSubstringsMatch	Да

9 Отличительное имя

9.1 Общие сведения

Отличительное имя (записи в каталоге) представляет собой строку, сформированную из последовательности относительных отличительных имен RDN (Relative Distinguished Name) данной записи и каждой из вышестоящих записей. Имя RDN представляет собой совокупность одной или нескольких пар «тип атрибута — значение», каждая из которых совпадает с отдельным значением отличительного атрибута, содержащегося в записи.

Распространено ошибочное мнение, что каждый поиск записи в каталоге использует атрибуты, входящие в состав отличительного имени. Но отличительное имя представляет собой всего лишь уникальный идентификатор в каталоге, и вести по нему поиск нельзя. В действительности поиск записей осуществляется по парам «тип атрибута — значение», хранящимся в самой записи.

9.2 Относительное отличительное имя

9.2.1 Общие сведения

В качестве относительного отличительного имени RDN часто используется идентификатор пользователя UID или общее имя CN. Так как в конкретном каталоге желательно представлять много понятий, то в каталогах, предназначенных для здравоохранения, важно иметь общие соглашения об уникальных именах. В соответствии с соглашениями, принятыми организацией W3C для обозначения пространств имен, такое уникальное имя RDN должно быть составлено из сочетания имени издателя, присвоившего имя, и идентификатора, используя знак двоеточия («:») в качестве разделителя, например:

ID=имя_издателя:ИД

При идентификации медицинских работников в качестве издателя выступает регуляторный орган, сертифицирующий их деятельность. Это позволяет каждой стране или региону присваивать отличительное имя издателю, представляющему страну, регион или медицинское профессиональное сообщество (например, общества врачей, стоматологов, провизоров). При этом предполагается, что каждый издатель ведет собственную систему уникальной идентификации. Если образуется цепочка идентификаторов, то в качестве разделителя идентификаторов используется знак точки («.»).

9.2.2 Медицинские работники

9.2.2.1 Идентификатор медицинского работника в каталоге

В каталоге должна использоваться такая идентификация медицинских работников, которая позволит учесть:

- наличие у работника нескольких сертифицируемых специальностей,
- наличие нескольких мест, где он может оказывать медицинскую помощь.

9.2.2.2 Идентификатор пользователя UID

Чтобы обеспечить учет наличия у медицинского работника нескольких сертифицируемых специальностей и нескольких мест, где он может оказывать медицинскую помощь, идентификатор пользователя UID должен быть составлен следующим образом:

UID = идентификатор издателя: присвоенный им национальный или региональный идентификатор медицинского работника

Конечно, это может привести к появлению в каталоге нескольких записей об одном и том же физическом лице. Однако идентификация медицинского работника в системе здравоохранения является неотъемлемой частью информационного взаимодействия при оказании медицинской помощи, поэтому целесообразно акцентировать, что лицо контролируется конкретным регуляторным органом и в каждый момент времени действует в соответствии с правилами, установленными этим органом.

9.2.2.3 Общее имя

В атрибуте общего имени CN (Common Name) должно быть указано официальное именование физического лица или организации. Чтобы гарантировать уникальность общего имени и в то же время сохранить его читаемость, общее имя медицинского работника должно быть составлено следующим образом:

Фамилия, имя и отчество, UID,

где значение атрибута UID образовано в соответствии с положениями подпункта 9.2.2.2.

При наличии у лица нескольких фамилий в атрибуте CN первой должна быть указана та фамилия, которую выберет это лицо. Если в разных удостоверениях личности, выданных лицу государством, указаны различные написания фамилии, имени и отчества, то должно быть указано то написание, с которым лицо зарегистрировано регуляторным органом здравоохранения.

Представление общего имени CN не должно содержать званий или профессиональных суффиксов (например, «д.м.н.» или «профессор»). Однако суффиксы, предназначенные для различения лиц с одинаковыми именованиями (к примеру, «мл.», «ст.», «2-й»), должны быть включены.

9.2.2.4 Многозначное общее имя

Атрибут общее имя CN может иметь дополнительные значения, представляющие предпочтительное или привычное именование лица.

9.2.3 Получатели медицинской помощи

9.2.3.1 Представление

Для регистрации в каталоге получателей медицинской помощи могут использоваться различные системы идентификации, включая обезличивание. Им могут присваиваться региональные идентификаторы, перекрестные идентификаторы, используемые в регистрах пациентов, а также идентификаторы, присваиваемые региональными информационными системами. Лицо может быть представлено

различными экземплярами объектов каталога. Должна быть обеспечена возможность указания в критериях поиска всех идентифицирующих атрибутов, предусмотренных в сегменте PID.

9.2.3.2 Идентификатор пользователя UID

Поскольку разным организациям и органам необходимо идентифицировать получателей медицинской помощи в собственной информационной среде и на своей территории, то идентификатор пользователя UID должен быть составлен следующим образом:

UID = идентификатор издателя: присвоенный им национальный, региональный или ведомственный идентификатор пациента или лица

Такой подход может привести к появлению в каталоге, предназначенном для здравоохранения, нескольких записей об одном и том же лице. Однако идентификация получателя медицинской помощи в системе здравоохранения является неотъемлемой частью информационного взаимодействия при оказании медицинской помощи, поэтому целесообразно акцентировать, что идентификатор лица назначен конкретной организацией или органом. За этим неизбежно последует необходимость использования служб поиска идентификаторов пациента, поэтому класс объектов, описывающий получателя медицинской помощи, должен содержать атрибуты, обеспечивающие подобный поиск. При анонимном получении медицинской помощи этими атрибутами могут быть обратимые или необратимые псевдонимы и кодируемые значения. Для выделения домашнего адреса можно использовать идентификатор места жительства либо как часть общего имени CN, либо как необязательный атрибут в классе HCConsumer.

9.2.3.3 Общее имя CN

В атрибуте общего имени CN (Common Name) должно быть указано официальное именование физического лица или организации. Чтобы гарантировать уникальность общего имени и в то же время сохранить его читаемость, общее имя медицинского работника должно быть составлено следующим образом:

Фамилия, имя и отчества, UID

где значение атрибута UID образовано в соответствии с положениями подпункта 9.2.2.2.

При наличии у лица нескольких фамилий в атрибуте CN первой должна быть указана та фамилия, которую выберет это лицо. При этом суффиксы, предназначенные для различения лиц с одинаковыми именованиями (к примеру, «мл.», «ст.», «2-й»), должны быть включены.

9.2.3.4 Многозначное общее имя

Атрибут общее имя CN может иметь дополнительные значения, представляющие предпочтительное или привычное именование лица.

9.2.4 Организация

9.2.4.1 Идентификатор пользователя UID

Идентификатор пользователя UID, присваиваемый организации, должен быть составлен следующим образом:

UID = идентификатор издателя: присвоенный им национальный или региональный идентификатор организации

Такой подход может привести к появлению в каталоге, предназначенном для здравоохранения, нескольких записей об одной и той же организации. Однако идентификация организации в системе здравоохранения является неотъемлемой частью информационного взаимодействия при оказании медицинской помощи, поэтому целесообразно акцентировать, что идентификатор организации назначен конкретным органом.

9.2.4.2 Общее имя CN

В атрибуте общего имени CN (Common Name) должно быть указано текущее официальное наименование организации.

9.2.4.3 Сохранение юридического наименования организации

В случае поглощения, изменения наименования или иной реорганизации правопреемник должен быть указан в атрибуте DN вновь созданной записи с текущим юридическим наименованием. После закрытия организации в соответствующей записи заполняется атрибут даты закрытия HcClosureDate.

9.2.5 Роли/обязанности

9.2.5.1 Общие сведения

Поскольку пользователь с одним и тем же идентификатором UID может иметь несколько работ или обязанностей в системе здравоохранения, то этот тип классов объектов должен быть привязан к общему имени (CN). Тем самым значение атрибута CN используется в качестве относительного отличительного имени (RDN) любого класса объектов, описывающего данное понятие.

Таким образом, атрибут RDN роли будет иметь значение общего имени (CN). В случае роли, описываемой классом HCStandardRole, это имя должно быть составлено, используя стандартные структурные роли.

9.2.5.2 Класс HCOrganizationalRole

Класс HCOrganizationalRole используется для представления специальной структурной роли, описывающей обязанности и должность. Он предназначен не для обеспечения управления полномочиями, а для представления контактной информации и атрибутов, зависящих от выполняемых обязанностей. Общее имя роли должно быть составлено следующим образом:

CN.job_function@organization_domain_name

где CN — значение атрибута общего имени лица, а organization_domain_name — доменное имя организации, определенное в классе OrganizationalRole. Значение компонента job_function (обязанность) определяется структурой организации и занимаемой должностью.

9.2.5.3 Класс HCstandardRole

Класс HCstandardRole используется для описания стандартной структурной роли, которая может использоваться при управлении группами полномочий, основанном на применении каталога. Общее имя стандартной роли должно быть составлено следующим образом:

standardRole@organization_domain_name,

где standardRole — имя стандартной структурной роли, назначенной организацией, идентифицируемой доменным именем organization_domain_name, или

standardRole@Locality,

где standardRole — имя стандартной структурной роли, назначенной региональным органом Locality (например, органом штата).

9.2.5.4 Класс HClocalRole

Класс HClocalRole используется для описания новой, нестандартной структурной роли, определенной на региональном или местном уровне. Общее имя нестандартной роли должно быть составлено следующим образом:

localRole@organization_domain_name,

где localRole — имя нестандартной структурной роли, назначенной организацией, идентифицируемой доменным именем organization_domain_name, или

localRole @Locality,

где localRole — имя нестандартной структурной роли, назначенной региональным органом Locality (например, органом штата).

Приложение А
(справочное)

Сценарии использования каталогов, предназначенных для здравоохранения

А.1 Введение

В настоящем приложении представлен ряд общих примеров («сценариев»), описывающих общие деловые и технические требования к службам каталога, предназначенным для обеспечения информационного взаимодействия между различными секторами отрасли здравоохранения. Вначале приведены общие требования, касающиеся основных принципов обеспечения конфиденциальности и информационной безопасности и фундаментальных потребностей отрасли здравоохранения. Затем каждый сценарий детализируется следующим образом:

a) приводится описание сценария или ситуации, возникающей при оказании медицинской помощи и требующей использования служб каталога, предназначенного для здравоохранения;

b) формулируются итоговые деловые и технические требования к службам каталога.

А.2 Детализация сценариев

Сценарии, описанные в разделе А.3, демонстрируют возможные применения служб каталога при информационном взаимодействии в здравоохранении. Каждый сценарий предназначен для описания потенциального применения служб каталога при обеспечении безопасности информационного взаимодействия, требуемого при непосредственном оказании медицинской помощи, при выполнении административных функций, а также функций защиты информации. В силу распределенного характера оказания медицинской помощи во всем мире и необходимости активной кооперации разных лиц и организаций, обеспечивающей преемственную медицинскую помощь, любая служба каталога должна быть способна предоставлять свои услуги широкому спектру организаций здравоохранения, включая государственные, муниципальные и частные больницы и поликлиники.

А.3 Службы каталога, используемые в сценариях

Службы, используемые в сценариях применения каталога при информационном взаимодействии в здравоохранении, перечислены в таблице А.1.

Таблица А.1 — Службы каталога, используемые в сценариях

Служба	Номер сценария															
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Обеспечение клинических функций		X	X	X	X	X	X	X				X	X	X	X	X
Обеспечение административных функций и управления медицинской информацией	X	X	X			X	X				X	X	X			
Обеспечение безопасности медицинской информации	X	X	X	X	X	X	X	X	X	X		X	X	X	X	X
Обеспечение оказания медицинской помощи		X			X			X				X	X			X
Контактная/медицинская информация физического лица	X	X	X	X	X	X		X			X	X	X	X	X	X
Контактная/медицинская информация системы	X	X					X					X	X			
Контактная/медицинская информация организации			X	X		X		X			X	X	X			
Извлечение открытых ключей для шифрования	X	X	X	X	X	X	X	X			X	X	X			
Проверка электронной подписи			X	X	X	X	X					X	X		X	
Проверка в списке отозванных сертификатов			X	X	X	X	X	X			X	X	X	X	X	X
Аутентификация								X				X	X	X		X

Окончание таблицы А.1

Служба	Номер сценария															
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Биометрическая ссылка								X								
Поддержка сертификации/публикации									X	X	X					

В таблице А.1 отражены следующие сценарии:

1) Обработка счетов на оплату лечения.
2) Направления на лабораторные анализы/получение результатов.
3) Электронные рецепты.
4) Распространение клинических руководств.
5) Санитарное просвещение.
6) Направление пациента к другому врачу.
7) Ведение долговременной медицинской карты.
8) Плановое ведение пациента.
9) Обеспечение процесса сертификации в УЦ.
10) Обеспечение процесса выдачи сертификатов атрибутов.
11) Обеспечение процесса наделения полномочиями.
12) Лечение пациента в другой стране.
13) Направление пациента на лечение из другой страны.
14) Дистанционный доступ к медицинскому программному обеспечению.
15) Делегирование полномочий.
16) Мобильная аутентификация пользователя.

А.4 Описание сценариев

А.4.1 Обработка счетов на оплату лечения

А.4.1.1 Описание сценария

В настоящем сценарии предложен пример использования служб каталога для обеспечения защищенного информационного взаимодействия при выполнении административных обязанностей. Информационная система учета оплаты лечения формирует файл с пакетом счетов на оплату оказанной медицинской помощи в соответствии с действующими правилами электронного обмена информацией. Эта система обращается к каталогу для извлечения коммуникационного адреса и открытого ключа получателя файла. Содержание файла шифруется этим ключом и передается получателю для обработки. Система обработки счетов, установленная у получателя, обрабатывает это сообщение и формирует протокол с указанием причин, по которым счета не могут быть немедленно оплачены. Затем она извлекает из каталога запись о медицинской организации, отправившей файл, объект EdiAdministrativeContact, идентифицирующий лицо, ответственное за администрирование электронного информационного взаимодействия, извлекает из этого объекта контактные данные лица и его сертификат открытого ключа, и передает протокол системе электронной почты. Зашифрованный протокол причин отказа в оплате передается по электронной почте контактной группе медицинской организации, которая запрашивает разъяснения и подтверждающую документацию у лечащего врача. Врач извлекает из медицинской информационной системы требуемую документацию о лечении субъекта медицинской помощи и посылает плательщику ответное зашифрованное сообщение электронной почты, содержащее эту документацию, взяв из каталога контактную информацию плательщика и сертификат открытого ключа шифрования.

А.4.1.2 Использование служб каталога

В этом сценарии каталог используется для получения контактной информации физического лица и системы, для отправки группе сообщения электронной почты, а также для извлечения открытых ключей, с помощью которых осуществляется шифрование.

А.4.2 Направления на лабораторные анализы/получение результатов

А.4.2.1 Описание сценария

В настоящем сценарии предложен пример использования служб каталога для обеспечения защищенного информационного взаимодействия медицинского работника с организацией.

Лечащий врач консультирует пациента и принимает решение о назначении лабораторных анализов. Затем он посылает по электронной почте зашифрованное письмо, адресованное лабораторной службе определенной медицинской организации, взяв из каталога необходимую контактную информацию и открытый ключ шифрования и подписав содержание письма своим закрытым ключом. Лаборатория выполняет требуемые исследования биоматериала пациента и по электронной почте отправляет результаты исследования направившей медицинской организации, опять-таки используя каталог для извлечения соответствующей контактной информации и открытого ключа шифрования. Перед отправкой результаты исследований подписываются персоналом лаборатории

и/или лабораторной информационной системой. Лечащий врач посылает пациенту подписанное и зашифрованное электронное письмо с результатами исследований, беря из каталога контактную информацию и ключ шифрования пациента.

А.4.2.2 Использование служб каталога

В этом сценарии каталог используется для получения контактной информации лиц, организации и системы, а также для извлечения открытых ключей шифрования.

А.4.3 Электронные рецепты

А.4.3.1 Описание сценария

В настоящем сценарии предложен пример использования служб каталога для обеспечения защищенного информационного взаимодействия и проверки электронной подписи в процессе выполнения медицинских функций. Врач выписывает электронный рецепт и подписывает его своим ключом электронной подписи. Перед подписью во избежание потенциальных профессиональных недоразумений осуществляется проверка, не числится ли сертификат этого ключа в списке отозванных сертификатов (СОС). Подписанный и зашифрованный рецепт передается в аптеку. При этом контактная информация аптеки и ее сертификат открытого ключа шифрования извлекаются из каталога LDAP. Фармацевт аутентифицируется в информационной системе аптеки, которая предоставляет ему расшифрованное сообщение, проверяет электронную подпись и содержание рецепта, извлекая открытый ключ из каталога LDAP. С помощью вызова служб каталога осуществляются проверки, что сертификат электронной подписи не отозван и что он был издан доверенным УЦ. Если для проверки действительности сертификата используется служба OCSP, то ее идентификатор также извлекается из каталога.

А.4.3.2 Использование служб каталога

В этом сценарии каталог используется для получения контактной информации лица и организации, а также для извлечения открытых ключей шифрования и проверки электронной подписи и проверки отсутствия идентификатора сертификата в СОС.

А.4.4 Распространение клинических руководств

А.4.4.1 Описание сценария

В настоящем сценарии предложен пример использования служб каталога для обеспечения электронной рассылки информации врачам с учетом их профессиональной роли. Дополнение к клиническому руководству по лечению онихомикоза, посвященное новой лекарственной терапии в сочетании с традиционным незначительным хирургическим вмешательством, рассылается всем дерматологам. Каталог используется для идентификации группы всех дерматологов. Сообщение подписывается, и получатели в свою очередь используют каталог для проверки аутентичности подписи и действительности ее сертификата.

А.4.4.2 Использование служб каталога

В этом сценарии каталог используется для получения контактной информации лиц, а также для извлечения открытых ключей шифрования и проверки электронной подписи и проверки отсутствия идентификатора сертификата в СОС.

А.4.5 Санитарное просвещение

А.4.5.1 Описание сценария

В настоящем сценарии предложен пример использования служб каталога для обеспечения защищенной электронной передачи пациентам подписанной информации. После публикации дополнений к типовому плану ведения пациентов система ведения персональных электронных медицинских карт идентифицирует пациентов, планы ведения которых затрагивают эти дополнения, извлекает из каталога контактную информацию и открытые ключи шифрования этих пациентов, а затем инициирует рассылку этим пациентам дополнений к планам ведения. Сообщения, направляемые им по электронной почте, подписываются и шифруются. Система электронной почты пациента обращается к каталогу для проверки действительности сертификата подписи, а затем проверяет подпись.

А.4.5.2 Использование служб каталога

В этом сценарии каталог используется для получения контактной информации лиц, а также для извлечения открытых ключей шифрования и проверки электронной подписи и проверки отсутствия идентификатора сертификата в СОС.

А.4.6 Направление пациента к другому врачу

А.4.6.1 Описание сценария

В настоящем сценарии предложен пример использования служб каталога для обеспечения защищенной электронной передачи данных, используя контактную информацию медицинского работника, имеющего несколько ролей в некоторой организации. Программа обработки направлений взаимодействует с каталогом для идентификации организации и получения контактной информации медицинского работника, которому адресована информация о направлении пациента. В данном сценарии медицинский работник имеет две роли в организации — получателе направления — административную и клиническую. Чтобы отправить сообщение по правильному адресу, в каталоге осуществляется поиск адреса электронной почты объекта, у которого значение атрибута objectClass равно HcOrganizationalRole, значение атрибута roleOccupant равно отличительному имени DN медицинского работника, а значение атрибута общего имени CN равно заданному значению обязанностей job_function@organization. Вместо этого можно выполнить два поиска: сначала найти все обязанности job_function медицинского работника в данной организации, а затем извлечь контактную информацию, связанную с требуемой обязанностью. Коммуникационный адрес и сертификат шифрования извлекаются с помощью запроса к каталогу LDAP, и программа обработки

направлений посылает подписанное уведомление и указания по лечению пациента получателю направления. Организация-получатель обращается к каталогу для проверки действительности сертификата подписи, а затем проверяет подпись.

А.4.6.2 Использование служб каталога

В этом сценарии каталог используется для получения контактной информации лица, организации, а также для извлечения открытых ключей шифрования и проверки электронной подписи, поиска организации и проверки отсутствия идентификатора сертификата в СОС.

А.4.7 Ведение долговременной медицинской карты

А.4.7.1 Описание сценария

В настоящем сценарии предложен пример использования служб каталога для обеспечения защищенной электронной передачи информированного согласия пациента, заверенного электронной подписью. Пациент обращается к врачу для получения первичной, амбулаторной или неотложной помощи. В соответствии с региональной политикой необходимо получить информированное согласие пациента на просмотр ранее собранной медицинской информации, ее использование или раскрытие. Пациент подписывает информированное согласие на просмотр его медицинских карт. Соответствие содержания согласия и подписи проверяется с помощью извлечения открытого ключа из каталога LDAP. Проверяется, что сертификат подписи не отозван.

Система ведения долговременной медицинской карты извлекает из каталога информацию о системе ведения главного регистра пациентов, и обращается к ней для получения идентификаторов систем, от которых можно получить детальную медицинскую информацию о пациенте. Коммуникационные адреса и сертификаты шифрования этих систем извлекаются из каталога LDAP, и запрос детальной информации о пациенте направляется по адресам, указанным в атрибутах ClinicalInformationContact.

К врачу мог обратиться пациент, не имеющий возможности заверять документы своей электронной подписью. В соответствии с региональной политикой должно быть получено его информированное согласие на просмотр ранее собранной медицинской информации, ее использование или раскрытие.

А.4.7.2 Использование служб каталога

В этом сценарии каталог используется для получения адреса главного регистра пациентов, для проверки отсутствия идентификатора сертификата электронной подписи в СОС, а также для извлечения открытых ключей шифрования и поиска контактной информации.

А.4.8 Плановое ведение пациента

А.4.8.1 Описание сценария

В настоящем сценарии предложен пример использования служб каталога для аутентификации лица при доступе к персональной медицинской карте и для проверки уведомлений, заверенных электронной подписью. Для ввода результатов регулярных измерений пациент аутентифицируется системой ведения персональных медицинских карт с помощью ввода имени пользователя и пароля или цифрового сертификата. В последнем случае осуществляется проверка наличия идентификатора сертификата в СОС. Для проверки идентичности пациента может также использоваться вторичная биометрическая верификация. Автоматизированная система или лицо, ответственное за обработку введенных результатов измерений, создают и отправляют пациенту шифрованные уведомления о том, что пациенту запланирован прием к врачу, что пациент пропустил очередной прием, и т.д. Контактная информация пациентов и сертификаты шифрования извлекаются с помощью запроса к каталогу LDAP.

А.4.8.2 Использование служб каталога

В этом сценарии каталог используется для получения контактной информации лица, аутентификации, обращения к службе биометрической верификации, а также для извлечения открытых ключей шифрования и проверки отсутствия идентификатора сертификата в СОС.

А.4.9 Обеспечение процесса сертификации в УЦ

А.4.9.1 Описание сценария

В настоящем сценарии предложен пример использования служб каталога при управлении ключами и проверке действительности сертификатов в инфраструктуре открытых ключей. Каталог, используемый удостоверяющим центром, функционирующим для нужд системы здравоохранения, содержит иерархию УЦ и контактную информацию УЦ. Удостоверяющий центр выпускает сертификат для участника системы здравоохранения. В каталог вносятся сведения о субъекте сертификата, включая стандартные атрибуты и те, что предусмотрены схемой, специфичной для здравоохранения. УЦ отправляет в каталог открытые ключи и сертификаты, предназначенные для подписи, аутентификации и шифрования. Кроме того, УЦ обновляет СОС, хранящийся в каталоге.

А.4.9.2 Использование служб каталога

Каталог используется для хранения идентификации владельца сертификата и его контактной информации. Кроме того, он используется для хранения и извлечения выпущенных сертификатов, контактной информации УЦ и списков отозванных сертификатов.

А.4.10 Обеспечение процесса выдачи сертификатов атрибутов

А.4.10.1 Описание сценария

В настоящем сценарии предложен пример использования служб каталога при выпуске и отзыве сертификатов атрибута, ассоциированных с участником системы здравоохранения. Каталог, используемый органом по присвоению атрибутов (ОА), содержит иерархию ОА и контактную информацию ОА. Орган по присвоению атрибутов выпускает сертификат атрибута для участника системы здравоохранения. В информацию о субъекте сертификата,

хранящуюся в каталоге, вносятся сведения об атрибуте, заверенном этим сертификатом. ОА отправляет сертификат атрибута в каталог для размещения в записи о владельце сертификата или в объекте OrganizationalRole, связанном с владельцем. Кроме того, ОА обновляет СОС, хранящийся в каталоге.

А.4.10.2 Использование служб каталога

Каталог используется для хранения и извлечения выпущенных сертификатов, контактной информации ОА и списков отозванных сертификатов.

А.4.11 Обеспечение процесса наделения полномочиями

А.4.11.1 Описание сценария

В настоящем сценарии предложен пример использования служб каталога для доступа к атрибутам, используемым для проверки полномочий медицинского работника в системе здравоохранения. Медицинская организация или регуляторный орган, осуществляющий сертификацию медицинских работников, извлекает из каталога информацию об образовании и контактную информацию работника. Они могут также отправить в каталог содержание сертификата специалиста в форме сертификата атрибута.

А.4.11.2 Использование служб каталога

Каталог используется для хранения и извлечения детальной информации об образовании и полномочиях лица в системе здравоохранения.

А.4.12 Лечение пациента в другой стране

А.4.12.1 Описание сценария

В настоящем сценарии предложен пример использования служб каталога при принятии решения о представлении трансграничного доступа. Пациент заболел в другой стране и обратился к местному врачу. Этот врач входит в информационную систему местной медицинской организации, предъявив сертификат, выданный в данной стране. Сертификат проверяют, используя службы местного каталога и местный СОС. Затем врач отправляет участковому врачу страны проживания пациента зашифрованное сообщение, содержащее запрос на предоставление информации из медицинской карты и сертификат, заверяющий полномочия местного врача в стране пребывания пациента. Эти полномочия и действительность сертификата проверяются по каталогу страны пребывания.

А.4.12.2 Использование служб каталога

В этом сценарии каталог используется для получения контактной информации лица, а также для извлечения открытых ключей шифрования и проверки электронной подписи, поиска организации и проверки отсутствия идентификатора сертификата в СОС.

А.4.13 Направление пациента на лечение из другой страны

А.4.13.1 Описание сценария

В настоящем сценарии предложен пример использования служб каталога для поиска врачей конкретной специальности в другой стране и для обеспечения защищенного информационного взаимодействия с выбранным врачом, необходимого при оказании медицинской помощи. Пациент, находясь в другой стране, запрашивает у своего участкового врача направление на лечение в стране пребывания. Участковый врач аутентифицируется в местном каталоге и запрашивает получение информации о врачах требуемой специальности из каталога страны пребывания пациента. Выбрав специалиста, участковый врач аутентифицируется в местной системе электронной коммуникации, предъявляя полномочия, проверяемые по местному каталогу. Если эти полномочия достаточны, то создается сообщение направления на лечение к выбранному специалисту, заверяемое с помощью сертификата электронной подписи участкового врача. Действительность полномочий специалиста проверяется по СОС. Действительность полномочий участкового врача проверяется по СОС.

А.4.13.2 Использование служб каталога

В этом сценарии каталог используется для получения контактной информации лица, а также для извлечения открытых ключей шифрования и проверки электронной подписи, поиска организации и проверки отсутствия идентификатора сертификата в СОС.

А.4.14 Дистанционный доступ к медицинскому программному обеспечению

А.4.14.1 Описание сценария

В настоящем сценарии предложен пример использования служб каталога для аутентификации лица и для предоставления полномочий, назначенных лицу, системе принятия решений об авторизации доступа. Медицинское программное обеспечение сконфигурировано таким образом, что для его вызова по протоколу SSL на стороне клиента должен быть предъявлен сертификат аутентификации, выпущенный доверенным УЦ и выданный пользователю на специальном токене. При аутентификации сертификат считывается с токена и программное обеспечение осуществляет поиск его содержания в каталоге пользователей. Если поиск успешен, то пользователь идентифицирован. Роли аутентифицированного пользователя извлекаются с помощью запроса к каталогу LDAP. Ролевое решение об авторизации доступа осуществляется с помощью списка ролей, назначенных группе, в которую входит пользователь, или на основании содержания сертификатов атрибута. Проверяется статус отзыва сертификатов, и пользователю разрешается доступ в соответствии с полномочиями на вызов данного медицинского программного обеспечения.

А.4.14.2 Использование служб каталога

Каталог используется для аутентификации ролевой информации пользователя в целях принятия решений системой ролевого контроля доступа. Он также используется для проверки отсутствия идентификатора сертификата в СОС.

А.4.15 Делегирование полномочий

А.4.15.1 Описание сценария

В настоящем сценарии предложен пример использования служб каталога для передачи сертификатов атрибута и статуса отзыва сертификата в целях принятия решения об авторизации. Медицинский работник с помощью сертификата атрибута делегирует право при определенных условиях действовать от его имени. Проверка пути к сертификату и статуса его отзыва осуществляются с помощью обращения к каталогу.

А.4.15.2 Использование служб каталога

Каталог используется для проверки права делегирования полномочий и отсутствия идентификатора сертификата в СОС.

А.4.16 Мобильная аутентификация пользователя

А.4.16.1 Описание сценария

В настоящем сценарии предложен пример использования служб каталога для аутентификации пользователя с помощью сертификатов X.509 и проверки действительности этих сертификатов. Пользователь с помощью мобильного устройства предъявляет информационной системе сертификат аутентификации. Проверяется статус отзыва сертификата. Затем информационная система запрашивает у пользователя имя и пароль и проверяет введенные данные, обращаясь к каталогу.

А.4.16.2 Использование служб каталога

Каталог используется для аутентификации пользователя, а также для проверки отсутствия идентификатора сертификата в СОС и проверки пароля.

Приложение В
(справочное)

Ссылочные классы объектов

В.1 Класс inetOrgPerson

Источник	Класс inetOrgPerson описан в документе RFC 2798
Класс объектов:	inetOrgPerson
Родительский класс:	organizationalPerson
ОИД:	2.16.840.1.113730.3.2.2
Тип класса объектов:	Структурный

Обязательные атрибуты описаны в таблице В.1, необязательные — в таблице В.2.

Таблица В.1 — Обязательные атрибуты класса inetOrgPerson

Атрибут	ОИД	Описание	Синтаксис	Правила сравнения	Кратный
sn	2.5.4.4	Фамилия	DirectoryString	caseIgnoreMatch	Да
cn	2.5.4.3	RFC 2256: общий супертип атрибутов именования	DirectoryString	caseIgnoreMatch	Да

Таблица В.2 — Необязательные атрибуты класса inetOrgPerson

Атрибут	ОИД	Описание	Синтаксис	Правила сравнения	Кратный
description	2.5.4.13	Описательная информация	DirectoryString	caseIgnoreMatch	Да
seeAlso	2.5.4.34	RFC 2256: общий супертип атрибутов DN	DistinguishedName	distinguishedNameMatch	Да
telephoneNumber	2.5.4.20	RFC 1274: телефонный номер	TelephoneNumber	telephoneNumberMatch	Да
userPassword	2.5.4.35	RFC 2256/2307: пароль пользователя	Octet String	octetStringMatch	Да
title	2.5.4.12	Должность (в отличие от титула)	DirectoryString	caseIgnoreMatch	Да
ou	2.5.4.11	Отличительное имя DN организации — основного места работы	DirectoryString	caseIgnoreMatch	Да
preferredDeliveryMethod	2.5.4.28	RFC 2256: предпочтительный метод доставки	1.3.6.1.4.1.1466.115.121.1.14		Нет
st	2.5.4.8	Штат или провинция	DirectoryString	caseIgnoreMatch	Да
telexNumber	2.5.4.21	Номер телекса	TelexNumber		Да
l	2.5.4.7	Наименование региона	DirectoryString	caseIgnoreMatch	Да
physicalDeliveryOfficeName	2.5.4.19	Наименование физического отделения доставки	DirectoryString	caseIgnoreMatch	Да
postalCode	2.5.4.17	Почтовый индекс	DirectoryString	caseIgnoreMatch	Да
internationalISDNNumber	2.5.4.25	RFC 2256: международный номер ISDN	NumericString	numericStringMatch	Да
x121Address	2.5.4.24	RFC 2256: адрес X.121	NumericString	numericStringMatch	Да

Продолжение таблицы В.2

Атрибут	ОИД	Описание	Синтаксис	Правила сравнения	Кратный
registeredAddress	2.5.4.26	RFC 1274: почтовый адрес	PostalAddress	caseIgnoreListMatch	Да
street	2.5.4.9	RFC 2256: адрес улицы места проживания данного субъекта	DirectoryString	caseIgnoreMatch	Да
postalAddress	2.5.4.16	RFC 1274: почтовый адрес	PostalAddress	caseIgnoreListMatch	Да
facsimileTelephoneNumber	2.5.4.23	RFC 2256: телефонный номер факсимильного устройства (факс)	FacsimileTelephoneNumber		Да
teletexTerminalIdentifier	2.5.4.22	RFC 2256: идентификатор телексного терминала	1.3.6.1.4.1.1466.115.121.1.51		Да
postOfficeBox	2.5.4.18	RFC 2256: почтовый ящик	DirectoryString	caseIgnoreMatch	Да
destinationIndicator	2.5.4.27	RFC 2256: признак места назначения	PrintableString	caseIgnoreMatch	Да
userCertificate	2.5.4.36	RFC 2256: двоичный сертификат пользователя в соответствии со спецификацией X.509	Certificate		Да
uid	0.9.2342.19200300.100.1.1	RFC 1274: идентификатор пользователя	DirectoryString	caseIgnoreMatch	Да
homePostalAddress	0.9.2342.19200300.100.1.39	RFC 1274: почтовый адрес дома	PostalAddress	caseIgnoreListMatch	Да
employeeType	2.16.840.1.113730.3.1.4	RFC 2798: тип занятости лица	DirectoryString	caseIgnoreMatch	Да
preferredLanguage	2.16.840.1.113730.3.1.39	RFC 2798: письменный или устный язык общения, предпочтительный для данного лица	DirectoryString	caseIgnoreMatch	Нет
mail	0.9.2342.19200300.100.1.3	RFC 1274: почтовый ящик в формате RFC 822	IA5String	caseIgnoreIA5Match	Да
homePhone	0.9.2342.19200300.100.1.20	RFC 1274: номер домашнего телефона	TelephoneNumber	telephoneNumberMatch	Да
roomNumber	0.9.2342.19200300.100.1.6	RFC 1274: номер комнаты	DirectoryString	caseIgnoreMatch	Да
x500UniqueIdentifier	2.5.4.45	RFC 2256: уникальный идентификатор в каталоге X.500	BitString	bitStringMatch	Да
employeeNumber	2.16.840.1.113730.3.1.3	RFC 2798: числовой идентификатор работника в организации	DirectoryString	caseIgnoreMatch	Нет
photo	0.9.2342.19200300.100.1.7	RFC 1274: фотография (факс G3)	1.3.6.1.4.1.1466.115.121.1.23		Да
businessCategory	2.5.4.15	RFC 2256: категория деловой активности	DirectoryString	caseIgnoreMatch	Да
pager	0.9.2342.19200300.100.1.42	RFC 1274: телефонный номер пейджера	TelephoneNumber	telephoneNumberMatch	Да

Окончание таблицы В.2

Атрибут	ОИД	Описание	Синтаксис	Правила сравнения	Кратный
o	2.5.4.10	RFC2256: наименование организации (общий супертип атрибутов именования)	DirectoryString	caseIgnoreMatch	Да
jpegPhoto	0.9.2342.19200300.100.1.60	RFC 2798: изображение в формате JPEG	JPEG		Да
secretary	0.9.2342.19200300.100.1.21	RFC 1274: отличительное имя (DN) секретаря	DN	distinguishedNameMatch	Да
audio	0.9.2342.19200300.100.1.55	RFC 1274: аудио (в формате u-law)	Audio		Да
userPKCS12	2.16.840.1.113730.3.1.216	RFC 2798: PKCS #12 личный идентификатор пользователя в соответствии с синтаксисом PFX PDU	Binary		Да
displayName	2.16.840.1.113730.3.1.241	RFC 2798: предпочтительное наименование при выводе содержания записей	DirectoryString	caseIgnoreMatch	Нет
mobile	0.9.2342.19200300.100.1.41	RFC 1274: номер мобильного телефона	TelephoneNumber	telephoneNumberMatch	Да
labeledURI	1.3.6.1.4.1.250.1.57	RFC 2079: унифицированный идентификатор ресурса с дополнительным элементом	DirectoryString	caseExactMatch	Да
carLicense	2.16.840.1.113730.3. 1.1	RFC 2798: лицензия или регистрационный номер транспортного средства	DirectoryString	caseIgnoreMatch	Да
givenName	2.5.4.42	RFC 2256: общий генерализованный тип имен лица	DirectoryString	caseIgnoreMatch	Да
Manager	0.9.2342.19200300.100.1.10	RFC 1274: отличительное имя (DN) управляющего	DN	distinguishedNameMatch	Да
userSMIMECertificate	2.16.840.1.113730.3.1.40	RFC 2798: PKCS#7 подписанные данные, используемые для поддержки S/MIME	Binary		Да
userSMIMECertificate	2.16.840.1.113730.3.1.40	RFC 2798: PKCS#7 подписанные данные, используемые для поддержки S/MIME	Binary		Да
departmentNumber	2.16.840.1.113730.3.1.2	RFC 2798: идентификация отдела в организации	DirectoryString	caseIgnoreMatch	Да

В.2 Класс Organization

Источник	Класс Organization описан в документе X.521 (ИСО/МЭК 9594-7)
Класс объектов:	Organization
Родительский класс:	Top
ОИД:	2.5.6.4
Тип класса объектов:	Структурный

Обязательные атрибуты описаны в таблице В.3, необязательные — в таблице В.4.

Таблица В.3 — Обязательные атрибуты класса Organization

Атрибут	ОИД	Описание	Синтаксис	Правила сравнения	Кратный
o	2.5.4.10	RFC 2256: наименование организации (общий супертип атрибутов именования)	DirectoryString	caseIgnoreMatch	Да

Таблица В.4 — Необязательные атрибуты класса Organization

Атрибут	ОИД	Описание	Синтаксис	Правила сравнения	Кратный
description	2.5.4.13	Описательная информация	DirectoryString	caseIgnoreMatch	Да
preferredDelivery-Method	2.5.4.28	RFC 2256: предпочтительный метод доставки	1.3.6.1.4.1.1466.115.121.1.14		Нет
searchGuide	2.5.4.14	RFC 2256: вместо атрибута searchGuide следует использовать атрибут enhancedSearchGuide	1.3.6.1.4.1.1466.115.121.1.25		Да
st	2.5.4.8	RFC 2256: штат или провинция	DirectoryString	caseIgnoreMatch	Да
businessCategory	2.5.4.15	RFC 2256: вид деятельности	DirectoryString	caseIgnoreMatch	Да
telexNumber	2.5.4.21	Номер телекса	TelexNumber		Да
l	2.5.4.7	Наименование региона	DirectoryString	caseIgnoreMatch	Да
seeAlso	2.5.4.34	RFC 2256: общий супертип атрибутов DN	Distinguished-Name	distinguished-NameMatch	Да
telephoneNumber	2.5.4.20	RFC 1274: телефонный номер	TelephoneNum-ber	telephoneNum-berMatch	Да
physicalDeliveryOffi-ceName	2.5.4.19	Наименование физического отделения доставки	DirectoryString	caseIgnoreMatch	Да
postalCode	2.5.4.17	Почтовый индекс	DirectoryString	caseIgnoreMatch	Да
internationalISDN-Number	2.5.4.25	RFC 2256: международный номер ISDN	NumericString	numericString-Match	Да
x121Address	2.5.4.24	RFC 2256: адрес X.121	NumericString	numericString-Match	Да
userPassword	2.5.4.35	RFC 2256/2307: пароль пользователя	Octet String	octetStringMatch	Да
registeredAddress	2.5.4.26	RFC 1274: почтовый адрес	PostalAddress	caseIgnoreList-Match	Да
street	2.5.4.9	RFC 2256: адрес улицы места проживания данного субъекта	DirectoryString	caseIgnoreMatch	Да
postalAddress	2.5.4.16	RFC 1274: почтовый адрес	PostalAddress	caseIgnoreList-Match	Да
facsimileTelephone Number	2.5.4.23	RFC 2256: телефонный номер факсимильного устройства (факс)	FacsimileTele-phoneNumber		Да
teletexTerminalIden-tifier	2.5.4.22	RFC 2256: идентификатор телексного терминала	1.3.6.1.4.1.1466.115.121.1.51		Да

Окончание таблицы В.4

Атрибут	ОИД	Описание	Синтаксис	Правила сравнения	Кратный
postOfficeBox	2.5.4.18	RFC 2256: почтовый ящик	DirectoryString	caseIgnoreMatch	Да
destinationIndicator	2.5.4.27	RFC 2256: признак места назначения	PrintableString	caseIgnoreMatch	Да

В.3 Класс organizationalRole

Класс объектов:	organizationalRole
Родительский класс:	Top
ОИД:	2.5.6.8
Тип класса объектов:	Структурный

Обязательные атрибуты описаны в таблице В.5, необязательные — в таблице В.6.

Таблица В.5 — Обязательные атрибуты класса organizationalRole

Атрибут	ОИД	Описание	Синтаксис	Правила сравнения	Кратный
cn	2.5.4.3	RFC 2256: общее имя (общий супертип атрибутов именования)	DirectoryString	caseIgnoreMatch	Да

Таблица В.6 — Необязательные атрибуты класса organizationalRole

Атрибут	ОИД	Описание	Синтаксис	Правила сравнения	Кратный
description	2.5.4.13	Описательная информация	DirectoryString	caseIgnoreMatch	Да
ou	2.5.4.11	Отличительное имя DN организации — основного места работы	DirectoryString	caseIgnoreMatch	Да
preferredDelivery-Method	2.5.4.28	RFC 2256: предпочтительный метод доставки	1.3.6.1.4.1.1466.115.121.1.14		Нет
st	2.5.4.8	Штат или провинция	DirectoryString	caseIgnoreMatch	Да
telexNumber	2.5.4.21	Номер телекса	TelexNumber		Да
l	2.5.4.7	Наименование региона	DirectoryString	caseIgnoreMatch	Да
seeAlso	2.5.4.34	RFC 2256: общий супертип атрибутов DN	Distinguished-Name	distinguished-NameMatch	Да
telephoneNumber	2.5.4.20	RFC 1274: телефонный номер	TelephoneNum-ber	telephoneNum-berMatch	Да
physicalDeliveryOffi-ceName	2.5.4.19	Наименование физического отделения доставки	DirectoryString	caseIgnoreMatch	Да
postalCode	2.5.4.17	Почтовый индекс	DirectoryString	caseIgnoreMatch	Да
roleOccupant	2.5.4.33	RFC 2256: общий супертип атрибутов DN	Distinguished-Name	distinguished-NameMatch	Да
internationalISDN-Number	2.5.4.25	RFC 2256: международный номер ISDN	NumericString	numericString-Match	Да
x121Address	2.5.4.24	RFC 2256: адрес X.121	NumericString	numericString-Match	Да

Окончание таблицы В.6

Атрибут	ОИД	Описание	Синтаксис	Правила сравнения	Кратный
registeredAddress	2.5.4.26	RFC 1274: почтовый адрес	PostalAddress	caseIgnoreListMatch	Да
street	2.5.4.9	RFC 2256: адрес улицы места проживания данного субъекта	DirectoryString	caseIgnoreMatch	Да
postalAddress	2.5.4.16	RFC 1274: почтовый адрес	PostalAddress	caseIgnoreListMatch	Да
facsimileTelephoneNumber	2.5.4.23	RFC 2256: телефонный номер факсимильного устройства (факс)	FacsimileTelephoneNumber		Да
teletexTerminalIdentifier	2.5.4.22	RFC 2256: идентификатор телексного терминала	1.3.6.1.4.1.1466.115.121.1.51		Да
postOfficeBox	2.5.4.18	RFC 2256: почтовый ящик	DirectoryString	caseIgnoreMatch	Да
destinationIndicator	2.5.4.27	RFC 2256: признак места назначения	PrintableString	caseIgnoreMatch	Да

В.4 Класс GroupOfNames

Источник	Класс GroupOfNames описан в документе X.521 (ИСО/МЭК 9594-7)
Класс объектов:	GroupOfNames
Родительский класс:	Top
ОИД:	2.5.6.9
Тип класса объектов:	Структурный

Обязательные атрибуты описаны в таблице В.7, необязательные — в таблице В.8.

Таблица В.7 — Обязательные атрибуты класса GroupOfNames

Атрибут	ОИД	Описание	Синтаксис	Правила сравнения	Кратный
cn	2.5.4.3	RFC 2256: общее имя (общий супертип атрибутов именования)	DirectoryString	caseIgnoreMatch	Да
member	2.5.4.31	RFC 2256: общий супертип атрибутов DN	DistinguishedName	distinguishedNameMatch	Да

Таблица В.8 — Необязательные атрибуты класса GroupOfNames

Атрибут	ОИД	Описание	Синтаксис	Правила сравнения	Кратный
description	2.5.4.13	Описательная информация	DirectoryString	caseIgnoreMatch	Да
ou	2.5.4.11	Отличительное имя DN организации — основного места работы	DirectoryString	caseIgnoreMatch	Да
businessCategory	2.5.4.15	RFC 2256: категория деловой активности	DirectoryString	caseIgnoreMatch	Да
owner	2.5.4.32	RFC 2256: общий супертип атрибутов DN	DistinguishedName	distinguishedNameMatch	Да

Окончание таблицы В.8

Атрибут	ОИД	Описание	Синтаксис	Правила сравнения	Кратный
seeAlso	2.5.4.34	RFC 2256: общий супертип атрибутов DN	DistinguishedName	distinguishedNameMatch	Да
o	2.5.4.10	RFC 2256: наименование организации (общий супертип атрибутов именования)	DirectoryString	caseIgnoreMatch	Да

Приложение ДА
(справочное)

Сведения о соответствии ссылочных международных стандартов национальным стандартам Российской Федерации

Таблица ДА

Обозначение ссылочного международного стандарта	Степень соответствия	Обозначение и наименование соответствующего национального стандарта
ISO/HL7 27931:2009	—	*
* Соответствующий национальный стандарт отсутствует. До его утверждения рекомендуется использовать перевод на русский язык данного международного стандарта.		

Библиография

[1] ISO 7498-2, Information processing systems — Open Systems Interconnection — Basic Reference Model — Part 2: Security Architecture
[2] ISO/TS 14265, Health Informatics — Classification of purposes for processing personal health information
[3] ISO 17090 (all parts), Health informatics — Public key infrastructure
[4] ISO/TS 21298, Health informatics — Functional and structural roles
[5] ISO 27799, Health informatics — Information security management in health using ISO/IEC 27002
[6] ISO/TS 22600-2, Health informatics — Privilege management and access control — Part 2: Formal models
[7] ISO/IEC 2382-8, Information technology — Vocabulary — Part 8: Security
[8] ISO/IEC 10181-1, Information technology — Open Systems Interconnection — Security frameworks for open systems — Part 1: Overview
[9] ISO/IEC TR 13335-1, Information technology — Guidelines for the management of IT Security — Part 1: Concepts and models for IT Security[1)]
[10] ISO/IEC TR14516, Information technology — Security techniques — Guidelines for the use and management of Trusted Third Party services
[11] ISO/IEC 15945, Information technology — Security techniques — Specification of TTP services to support the application digital signatures
[12] ISO/IEC 27000, Information technology — Security techniques — Information security management systems — Overview and vocabulary
[13] ISO/IEC 27001, Information technology — Security techniques — Information security management systems — Requirements
[14] ISO/IEC 27005, Information technology — Security techniques — Information security risk management
[15] CWA 13896, Lightweight directory access protocol (LDAP) client profile
[16] CWA 13943: 2000, Lightweight directory access protocol (LDAP) V3: Level of support of LDAP server
[17] CWA 14193: 2001, Directory synchronisation and the meta-directory. An analysis of issues and techniques
[18] CWA 13678: 1999, Guidelines for naming in the directory
[19] Supplement DICOM 67: 2003, Configuration Management
[20] HL7 V3 RIM. Reference Information Model: Health Level Seven Inc., Ann Arbor HL7 V3, Entity Identification Service: Health Level Seven Inc., Ann Arbor
[21] IETF/RFC 2798: 2000, Definition of the inetOrgPerson LDAP Object Class
[22] IETF/RFC 3280: 2002, Internet X.509 Public Key Infrastructure Certificate and CRL Profile
[23] IETF/RFC 3377: 2002, Lightweight Directory Access Protocol (v3): Technical Specification
[24] IETF/RFC 3647: 2003, Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework
[25] IETF/RFC 3698: 2004, Lightweight Directory Access Protocol (LDAP): Additional Matching Rules
[26] IETF/RFC 3771: 2004, The Lightweight Directory Access Protocol (LDAP) Intermediate Response Message
[27] ITU-T Recommendation X.500: 2001 | ISO/IEC 9594-1, Information technology — Open Systems Interconnection — The Directory: Overview of concepts, models and services — Part 1[2)]
[28] ITU-T Recommendation X.501:2001 | ISO/IEC 9594-2, Information technology — Open Systems Interconnection — The Directory: Models — Part 2
[29] ITU-T Recommendation X.509:2001 | ISO/IEC 9594-8, Information technology — Open Systems Interconnection — The Directory — Public-key and attribute certificate frameworks — Part 8[3)]
[30] ITU-T Recommendation X.511:2001 | ISO/IEC 9594-3, Information technology — Open Systems Interconnection — The Directory: Abstract service definition — Part 3
[31] ITU-T Recommendation X.520:2001 | ISO/IEC 9594-6, Information technology — Open Systems Interconnection — The Directory: Selected attribute types — Part 6
[32] ITU-T Recommendation X.521:2001 | ISO/IEC 9594-7, Information technology — Open Systems Interconnection — The Directory: Selected object classes — Part 7
[33] ENV 13608-1, Health informatics — Security for healthcare communication — Concepts and terminology
[34] COBIT. (Control Objectives for Information and Related Technologies) — спецификация, разработанная организацией Information Systems Audit and Control Foundation

---

1) Отменен.

2) Документ X.500 является стандартом организации ITU-T, описывающим каталоги, используемые в них понятия, модели и службы.

3) Документ X.509 является стандартом организации ITU-T, описывающим сертификаты и их применение для аутентификации.

УДК 004:61:006.354 ОКС 35.240.80 П85 ОКСТУ 4002

Ключевые слова: здравоохранение, информатизация здоровья, электронная передача данных, тип данных, медицинская помощь, службы каталога

БЗ 7—2017/127

Редактор *М.В. Терекина*
Технический редактор *В.Н. Прусакова*
Корректор *М.И. Першина*
Компьютерная верстка *Е.О. Асташина*

Сдано в набор 22.06.2017. Подписано в печать 28.06.2017. Формат 60×84 1/8. Гарнитура Ариал.
Усл. печ. л. 5,58. Уч.-изд. л. 5,05. Тираж 19 экз. Зак. 1091.
Подготовлено на основе электронной версии предоставленной разработчиком стандарта

Издано и отпечатано во ФГУП «СТАНДАРТИНФОРМ», 123001 Москва, Гранатный пер., 4
www.gostinfo.ru info@gostinfo.ru