ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р ИСО/ТС 22600-2 — 2009

Информатизация здоровья

УПРАВЛЕНИЕ ПОЛНОМОЧИЯМИ И КОНТРОЛЬ ДОСТУПА

Часть 2

Формальные модели

ISO/TS 22600-2:2006
Health informatics — Privilege management and access control — Part 2: Formal models
(IDT)

Издание официальное

БЗ 8—2009/429

Москва
Стандартинформ
2010

gost.e-ecolog.ru

Предисловие

Цели и принципы стандартизации в Российской Федерации установлены Федеральным законом от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании», а правила применения национальных стандартов Российской Федерации — ГОСТ Р 1.0—2004 «Стандартизация в Российской Федерации. Основные положения»

Сведения о стандарте

1 ПОДГОТОВЛЕН Федеральным государственным учреждением «Центральный научно-исследовательский институт организации и информатизации здравоохранения Росздрава» (ЦНИИОИЗ Росздрава) и Государственным научным учреждением «Центральный научно-исследовательский и опытно-конструкторский институт робототехники и технической кибернетики» на основе собственного аутентичного перевода стандарта, указанного в пункте 4

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 468 «Информатизация здоровья» при ЦНИИОИЗ Росздрава — единоличным представителем ИСО ТК 215

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 14 сентября 2009 г. № 409-ст

4 Настоящий стандарт идентичен международному стандарту ИСО/ТС 22600-2:2006 «Информатизация здоровья. Управление полномочиями и контроль доступа. Часть 2. Формальные модели» (ISO/TS 22600-2.2006 «Health informatics — Privilege management and access control — Part 2: Formal models»)

5 ВВЕДЕН ВПЕРВЫЕ

Информация об изменениях к настоящему стандарту публикуется в ежегодно издаваемом информационном указателе «Национальные стандарты», а текст изменений и поправок — в ежемесячно издаваемых информационных указателях «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ежемесячно издаваемом информационном указателе «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

© Стандартинформ, 2010

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

Содержание

1 Область применения 1
2 Термины и определения 2
3 Парадигма компонентов 4
4 Базовые модели 5
4.1 Концептуальная структура 5
4.2 Модель зоны 6
4.3 Модель документа 8
4.4 Модель политики безопасности 8
4.5 Модель роли 11
4.6 Модель авторизации — назначение ролей и полномочий 12
4.7 Модель контроля 12
4.8 Модель делегирования 13
4.9 Модель контроля доступа 14
Приложение А (справочное) Функциональные и структурные роли 16
Приложение В (справочное) Примеры структурных ролей в здравоохранении 20
Библиография 21

Введение

В лечебно-профилактических учреждениях нередко внедряются информационные системы разных поставщиков, каждая из которых требует от пользователя отдельной аутентификации и авторизации доступа, поскольку они реализуют эти функции по-своему. Интеграция этих функций требует значительных затрат на взаимные отображения сведений о пользователях и организациях. В такой ситуации ресурсы, необходимые для разработки и эксплуатации функций обеспечения безопасности, растут в геометрической прогрессии с увеличением числа информационных систем.

С другой стороны, если рассматривать авторизацию с точки зрения учреждения здравоохранения, то будет очевидна потребность в гибкой модели ее реализации, поскольку в учреждениях постоянно происходят изменения. Одни подразделения закрываются, другие создаются, третьи объединяются.

Ситуация становится еще более сложной, когда для взаимодействия требуется пересечение периметров зон с разными политиками безопасности. Для преодоления различий между этими политиками необходимы взаимные соглашения о политиках между сторонами, обеспечивающими безопасность.

Другая сложность состоит в назначении пользователям ролей. Пользователь может исполнять различные роли в разное время и даже две или более роли одновременно. Например, пользователь может работать два месяца в роли медсестры, а следующие два — как акушерка, или же совмещать эти роли.

Более того, в учреждении здравоохранения могут быть идентифицированы разные обязанности в зависимости от выполняемой роли и рода деятельности пользователей. При переезде в другую страну или при переходе в другое медицинское учреждение для пользователей одних и тех же категорий может меняться тип или уровень авторизации, необходимой как для выполнения каких-либо действий, так и для получения доступа к информации.

Другой не менее важный актуальный вопрос — как повысить качество обслуживания, используя информационные технологии, не нарушая при этом прав личности пациента. Чтобы врачи могли получать наиболее адекватную информацию о пациенте, необходимо наличие «виртуальной электронной истории болезни», которая позволяла бы регистрировать всю медицинскую помощь, оказанную пациенту, независимо от того, где и кем она документировалась. При таком подходе необходима общая модель авторизации или специальное соглашение об авторизации между сторонами, обеспечивающими безопасность.

Кроме необходимости учета многообразия ролей и обязанностей, типичных для любой крупной организации, решающее значение имеют и другие аспекты медицинской помощи, например, этические или юридические, обусловленные особенностями используемой информации.

Необходимость в ограничительной авторизации актуальна и сейчас, но будет существенно возрастать в ближайшие два года в связи с увеличением обмена информацией между приложениями, чтобы удовлетворить потребность врачей в получении все большего и большего объема информации о пациенте в целях обеспечения высокого качества и эффективности лечения.

За последнее десятилетие произошли заметные изменения в части сервисов информационной безопасности прикладных программ и передачи данных. Ниже указаны некоторые факторы, способствующие этим изменениям:

- переход от централизованных систем на базе больших компьютеров к распределенным системам на базе местных вычислительных ресурсов;
- все больше данных хранится в информационных системах, и тем ценнее они для пользователей;
- пациенты становятся более мобильными, и их медицинские данные требуются в разных местах пребывания.

В связи с необходимостью защиты персональных данных, требуемой для исключения нежелательных личных и социальных последствий, эти изменения влекут за собой повышение требований к средствам защиты передачи и обработки медицинских данных. Эта защита должна распространяться как на обмен информацией, так и на ее обработку. Что касается таких механизмов защиты обмена данными, как аутентификация, целостность, конфиденциальность, доступность, отслеживаемость (включая трассируемость и невозможность отказа от авторства), контроль доступа к вычислительным ресурсам, а также службы удостоверения, именно аутентификация критична для большей части остальных механизмов. Это справедливо и по отношению к безопасности обработки данных, где необходимы управление доступом к данным и функциям программ, исполняемых на вышеуказанных вычислительных ресурсах, целостность, конфиденциальность, доступность, отслеживаемость, различимость и службы удостоверения.

Применение настоящего стандарта будет вызывать особую сложность в связи с тем, что участвующие стороны уже располагают действующими системами и не проявят особого желания немедленно обновить их или полностью заменить. Поэтому очень важно, чтобы стороны подписали соглашение о политике, в котором они подтверждают намерение к движению в сторону реализации настоящего стандарта по мере возникновения потребности в модификации этих систем.

Соглашение о политике должно также содержать описание выявленных различий в системах обеспечения информационной безопасности и согласованных мер по их преодолению. Например, в сервисе аутентификации права и обязанности одной стороны, запрашивающей доступ к информации другой стороны, должны обеспечиваться в соответствии с согласованной политикой, записанной в соглашении между сторонами. Для решения этой задачи необходимо обеспечить соответствующую группировку и классификацию как пользователей и поставщиков информации и информационных услуг, так и самой информации и предоставляемых услуг. Такая классификация может служить основой для реализации механизмов обработки требований доступа, категорирования информации и информационных услуг, а также механизмов описания политик контроля доступа и управления ими. Если все взаимодействующие стороны не видят каких-либо рисков, взаимодействие существующих систем и обмен информацией можно начинать сразу же после подписания соглашения о политике контроля доступа. Если риски настолько существенны, что их надо исключить до начала обмена информацией, то надо описать эти риски в соглашении о политике контроля доступа и добавить к нему перечень мероприятий по устранению рисков. Соглашение должно содержать график выполнения этих мероприятий и определять способ их финансирования.

Процесс документирования очень важен и служит основой для выработки соглашения о политике контроля доступа.

Требования к управлению полномочиями и контролю доступа предъявляются к сервисам защиты, необходимым для передачи медицинской информации и обеспечения распределенного доступа к этой информации. Настоящий стандарт представляет принципы и определяет сервисы, необходимые для управления полномочиями и контроля доступа. Криптографические протоколы не входят в область применения настоящего стандарта.

В стандарте ИСО/ТС 22600, состоящем из двух частей, содержатся ссылки на уже принятые стандарты информационной безопасности и архитектуры ее реализации, а также на спецификации, предложенные для здравоохранения такими организациями, как ИСО, CEN, ASTM, OMG, W3C и другими. В нем поддерживается применение подходящих стандартов, либо предлагается их улучшение или модификация, либо обосновывается необходимость разработки новых стандартов.

В ИСО/ТС 22600, часть 1 «Общие сведения и управление политикой», содержится описание сценариев и критичных характеристик трансграничного обмена информацией. В нем также приводятся примеры методов необходимого документирования, которые должны послужить основой соглашения о политике контроля доступа.

В настоящем стандарте (ИСО/ТС 22600, часть 2 «Формальные модели») содержатся более детальные описания архитектуры и моделей полномочий и управления полномочиями, реализуемых для обеспечения защиты совместного доступа к информации, дополненные примерами шаблонов соглашений о политике контроля доступа.

Настоящий стандарт тесно связан с другими международными стандартами в этой предметной области, например ИСО/ТС 17090 и ИСО/ТС 21091. Он также связан с ведущейся разработкой проекта ИСО/ТС 21298.

Распределенная архитектура совместно используемых медицинских информационных систем все в большей степени основана на применении вычислительных сетей. Благодаря ощутимым выгодам для пользователей, применение стандартизованных интерфейсов пользователя, инструментальных средств и протоколов, обеспечивающее платформенную независимость предлагаемых решений, становится все более популярным, что за пару последних лет привело к ощутимому росту числа действительно открытых информационных систем, предназначенных для функционирования в корпоративных вычислительных сетях и в частных виртуальных сетях.

Стандарт ИСО/ТС 22600 определяет сервисы управления полномочиями и контроля доступа, необходимые для распределенного доступа и обмена медицинской информацией между всеми заинтересованными пользователями, удаленными друг от друга и использующими разные средства защиты информации. В настоящем стандарте установлены принципы и определены сервисы, необходимые для управления полномочиями и контроля доступа. В нем определены необходимые понятия, базирующиеся на компонентах, и он предназначен для поддержки их технической реализации. Настоящий стандарт не определяет применение этих понятий в конкретных процессах оказания медицинской помощи.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Информатизация здоровья

УПРАВЛЕНИЕ ПОЛНОМОЧИЯМИ И КОНТРОЛЬ ДОСТУПА

Часть 2

Формальные модели

Health informatics. Privilege management and access control. Part 2. Formal models

Дата введения — 2010 — 07 — 01

1 Область применения

Назначением настоящего стандарта является обеспечение поддержки потребностей совместного доступа к медицинской информации различных административно независимых поставщиков медицинской помощи, учреждений здравоохранения, страховых медицинских организаций, их пациентов, персонала и коммерческих партнеров. Кроме того, настоящий стандарт предназначен для обеспечения поддержки запросов информации, поступающих как от отдельных лиц, так и от информационных систем.

В ИСО/ТС 22600, состоящем из двух частей, определены методы управления авторизацией и контроля доступа к данным и/или функциям. Он обеспечивает согласование политик контроля доступа и основан на концептуальной модели, по которой для управления доступом к информации, осуществляемым различными прикладными программами (программными компонентами), могут использоваться локальные серверы авторизации и службы распределенного каталога и репозитария политик контроля доступа. Репозитарий политик предоставляет информацию о правилах доступа к разным прикладным функциям, основанным на использовании ролей и других атрибутов. Служба каталога обеспечивает идентификацию отдельных пользователей. Предоставление доступа должно осуществляться на основе:

- аутентифицированной идентификации пользователя;
- правил доступа, относящихся к конкретному информационному объекту;
- правил относительно атрибутов авторизации, заданных менеджером авторизации для пользователя;
- функций конкретного приложения.

Настоящий стандарт в перспективе должен применяться как на локальном, так и на региональном или национальном уровне. Одним из ключевых моментов его применения является включение в письменное соглашение о политике контроля доступа организационных критериев и профилей авторизации, согласованных запрашивающими и предоставляющими доступ сторонами.

Настоящий стандарт поддерживает взаимодействие между несколькими менеджерами авторизации, которые могут действовать независимо от организационных и политических границ.

Правила взаимодействия определяются в соглашении о политике контроля доступа, подписанном всеми участвующими организациями, и служат основой для дальнейшей работы.

В качестве основы соглашения о политике контроля доступа предложен формат документации, дающий возможность получения сопоставимой документации от всех сторон, участвующих в обмене информацией.

Настоящий стандарт не включает в себя детали, связанные с конкретными платформами и реализациями. В нем не определяются сервисы и протоколы защиты технической передачи данных, определенные в других стандартах, например в ENV 13608, а также методы аутентификации.

Издание официальное

В данной части ИСО/ТС 22600 представлена базовая парадигма формальных высокоуровневых моделей архитектурных компонентов, основанных на ИСО/МЭК 10746. В данном контексте определены модель зоны, модель документа, модель политики, модель роли, модель авторизации, модель делегирования, модель управления и модель контроля доступа.

Определения даны с использованием метаязыков: Унифицированного языка моделирования (UML) и Расширяемого языка разметки (XML). Для разъяснения принципов использованы дополнительные диаграммы. Определения использованных атрибутов заимствованы из эталонной информационной модели HL7 и определений типов данных HL7.

2 Термины и определения

В настоящем стандарте применены следующие термины с соответствующими определениями:

2.1 **контроль доступа** (access control): Средства обеспечения доступа к ресурсам системы обработки данных только авторизованным субъектам авторизованными способами [7].

2.2 **отслеживаемость** (accountability): Свойство, обеспечивающее однозначную привязку действий субъекта к конкретному субъекту [8].

2.3 **уполномоченное лицо по атрибутам**; УЛА (attribute authority; AA): Уполномоченное лицо, назначающее полномочия путем выдачи сертификатов атрибутов.

2.4 **сертификат атрибута** (attribute certificate): Структура данных, заверенная цифровой подписью уполномоченного лица по сертификации, которая связывает некоторые значения атрибута с идентификацией его владельца.

2.5 **аутентификация** (authentication): Процесс достоверной идентификации субъектов информационной безопасности посредством надежной связи между идентификатором и его удостоверением.

Примечание — См. также аутентификацию источника данных и аутентификацию равноправного объекта.

2.6 **уполномоченное лицо** (authority): Субъект, ответственный за выдачу сертификатов.

Примечание — В настоящем стандарте определены две категории уполномоченных лиц: уполномоченное лицо по сертификации, выдающее сертификаты открытых ключей, и уполномоченное лицо по атрибутам, выдающее сертификаты атрибутов.

2.7 **авторизация** (authorization): Процесс предоставления прав, включая предоставление прав на доступ.

2.8 **доступность** (availability): Свойство быть доступным и годным к использованию по запросу авторизованного субъекта [8].

2.9 **подтверждение действительности сертификата** (certificate validation): Процесс установления того, что на настоящий момент сертификат является действительным, включая возможность создания и проверки пути сертификации, а также того, что на настоящий момент все сертификаты, выданные на данном пути, действительны (т.е. не просрочены и не отозваны).

2.10 **уполномоченное лицо по сертификации**; УС (certification authority; CA): Уполномоченное лицо, которому одна или несколько участвующих сторон доверили выпуск и присвоение сертификатов [10].

Примечания

1 Уполномоченное лицо по сертификации может факультативно создавать ключи для участвующих сторон.

2 Понятие «уполномоченное лицо» в термине «уполномоченное лицо по сертификации» означает всего лишь доверенную сторону, а не какую-либо государственную авторизацию. Более удачным термином может быть «издатель сертификата (cartificate issuer)», но термин «уполномоченное лицо по сертификации» очень широко употребляется.

2.11 **путь сертификации** (certification path): Упорядоченная последовательность сертификатов объектов в иерархическом каталоге, которая вместе с открытым ключом начального объекта пути позволяет получить сертификат окончательного объекта пути.

2.12 **конфиденциальность** (confidentiality): Свойство, заключающееся в том, что информация не может быть доступной или раскрытой для неавторизованных лиц, объектов или процессов [8].

2.13 **удостоверение** (credential): Предпосылка для назначения на роль или для подтверждения годности для роли.

2.14 **делегирование** (delegation): Передача полномочия от его обладателя другому объекту.

2.15 **путь делегирования** (delegation path): Упорядоченная последовательность сертификатов, которая вместе с аутентификацией личности заявителя полномочий позволяет проверить аутентичность полномочий заявителя.

2.16 **переменные среды** (environmental variables): Аспекты политики, необходимые для принятия решения об авторизации, которые не отражены в статических структурах, но доступны контролеру полномочий посредством локальных средств (например, время суток или текущий баланс счета).

2.17 **идентификация** (identification): Выполнение проверок, позволяющих системе обработки данных распознавать объекты.

2.18 **идентификатор** (identifier): Информационный объект, используемый для объявления идентичности до потенциального подтверждения соответствующим аутентификатором [18].

2.19 **целостность** (integrity): Свойство, удостоверяющее, что информация не изменена случайно или преднамеренно.

2.20 **ключ** (key): Последовательность символов, управляющая операциями шифрования и дешифровки [8].

2.21 **неоспоримость** (non-repudiation): Сервис, обеспечивающий подтверждение целостности и происхождения данных (неразрывно друг от друга) любой из участвующих сторон.

2.22 **политика** (policy): Комплекс юридических, политических, организационных, функциональных и технических обязательств по обмену информацией и совместной деятельности.

2.23 **соглашение о политике** (policy agreement): Письменное соглашение, в котором все участвующие стороны обязуются придерживаться определенного комплекса политик.

2.24 **принципал** (principal): Действующее лицо, способное реализовать определенные сценарии (пользователь, организация, система, устройство, прикладная программа, компонент, объект).

2.25 **секретный ключ** (private key): Ключ, используемый в асимметричном криптографическом алгоритме, обладание которым ограничено (обычно только одним субъектом) [12].

2.26 **полномочие** (privilege): Возможность, предоставленная объекту уполномоченным лицом в соответствии с атрибутом этого объекта.

2.27 **заявитель полномочий** (privilege asserter): Обладатель полномочий, использующий свой сертификат атрибута или сертификат открытого ключа для получения полномочий.

2.28 **инфраструктура управления полномочиями**; ИУП (privilege management infrastructure; PMI): Инфраструктура, способная поддерживать управление полномочиями для обеспечения развитой службы авторизации во взаимодействии с инфраструктурой открытых ключей.

2.29 **политика полномочий** (privilege policy): Политика, определяющая условия, при которых контролеры полномочий могут предоставлять/выполнять важные сервисы квалифицированным заявителям полномочий.

Примечание — Политика полномочий связана с атрибутами, ассоциированными с сервисом и с заявителями полномочий.

2.30 **контролер полномочий** (privilege verifier): Субъект, проверяющий сертификаты на соответствие политике полномочий.

2.31 **открытый ключ** (public key): Ключ, используемый в асимметричном криптографическом алгоритме, который может быть сделан общедоступным [12].

2.32 **сертификат открытого ключа**; СОК (public key certificate, PKC): Сертификат, обеспечивающий связь идентичности с открытым ключом.

Примечание — Идентичность может быть использована для поддержки принятия решений системой контроля доступа, основанной на идентификации, после того, как клиент подтвердит, что он имеет доступ к секретному ключу, соответствующему открытому ключу, содержащемуся в СОК.

2.33 **роль** (role): Комплекс способностей и/или действий, связанный с задачей.

2.34 **сертификат назначения роли** (role assignment certificate): Сертификат, содержащий атрибут роли, назначающий одну или более ролей держателю сертификата.

2.35 **сертификат роли** (role certificate): Сертификат, назначающий полномочия роли, а не напрямую отдельным лицам.

Примечание — Лица, назначенные на данную роль посредством сертификата атрибута или сертификата открытого ключа с расширением атрибутов каталога субъектов, содержащим данное назначение, косвенно получают полномочия, содержащиеся в сертификате роли.

2.36 **сертификат спецификации роли** (role specification certificate): Сертификат, содержащий назначение роли полномочий.

2.37 **важность** (sensitivity): Характеристика ресурса, выражающая его ценность или значимость.

2.38 **безопасность** (security): Сочетание доступности, конфиденциальности, целостности и отслеживаемости [18].

2.39 **политика безопасности** (security policy): Утвержденный план или способ действий по обеспечению информационной безопасности.

2.40 **сервис безопасности** (security service): Сервис, предоставляемый уровнем взаимодействия открытых систем, обеспечивающий надлежащую степень безопасности систем или передачи данных [8].

2.41 **поставщик полномочий**; ПОП (source of authority, SOA): Уполномоченное лицо по атрибутам (см. 2.3), которому контролер полномочий доступа к определенному ресурсу доверяет как единственному лицу, уполномоченному назначать ряд полномочий.

2.42 **цель** (target): Ресурс, к которому субъект запрашивает доступ.

Примечание — Важность цели моделируется в настоящем стандарте как набор атрибутов, представленных либо атрибутами в нотации ASN.1, либо элементами XML.

2.43 **доверие** (trust): Качество, при наличии которого о субъекте говорят, что он «оказывает доверие» другому субъекту, когда он (первый субъект) предполагает, что второй субъект будет действовать в полном соответствии с ожиданиями первого субъекта.

Примечание — Понятие доверия может относиться только к некоторой конкретной функции. Ключевая роль доверия в данном контексте состоит в описании взаимосвязи между аутентифицирующимся субъектом и уполномоченным лицом; субъект должен быть уверен, что он может доверять тому, что уполномоченное лицо создает только действительные и надежные сертификаты.

3 Парадигма компонентов

Архитектура перспективной медицинской информационной системы базируется на модели базовых компонентов, разработанной в середине 90-х годов (например, см. [1], [2], [3]). Основами этой архитектуры служат базовая информационная модель (БИМ) и согласованные словари данных, способствующие обеспечению взаимной приемлемости. Основываясь на них, будут определены специфичные для конкретных предметных областей модели ограничений, представляющие специфичные для конкретных предметных областей концепции знаний, включая как структурные, так и функциональные знания. Соответствующие компоненты должны быть созданы в соответствии со всеми точками зрения на базовую модель открытой распределенной обработки (БМ-ОРО) [20], т. е. предпринимательской, информационной, вычислительной, инженерной и технологической точками зрения. Точка зрения фокусирует внимание на одном аспекте, абстрагируясь от всех остальных. Разные концепции предметной области и представление их точек зрения входят в задачи не программистов, а экспертов предметной области. Поэтому они используют соответствующие средства выражения, в том числе специальные графические представления (например, UML-диаграммы), а иногда даже словесные шаблоны, выраженные на языке XML.

Компоненты могут быть агрегированы в более высокоуровневые композиции. В противоположность определению примитивов и композиций ИСО, в модели базовых компонентов выделены, по крайней мере, четыре уровня композиции/декомпозиции (см. рисунок 1).

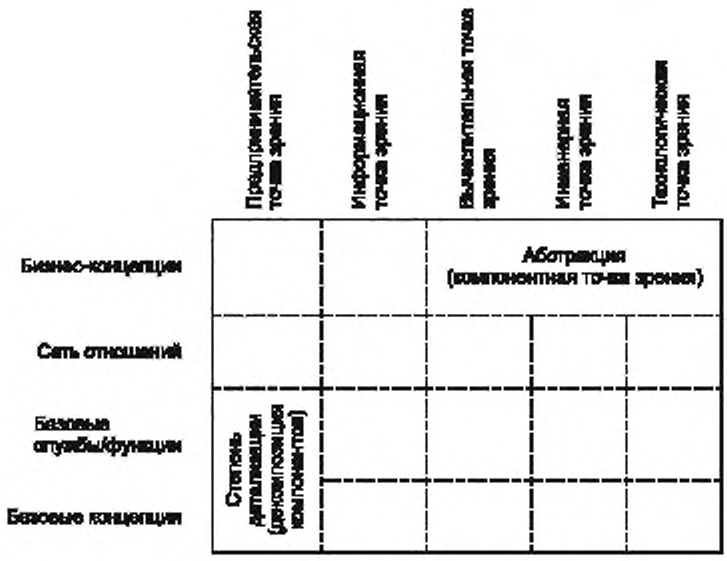

Рисунок 1 — Общая компонентная модель

Агрегирование осуществляется исходя из знаний, связанных с содержанием или процессами и выраженных логическими схемами/алгоритмами/операциями или правилами/потоками работ/процедурами/взаимосвязями. Таким образом, агрегирование составных частей «моделей ограничений» управляется вышеупомянутыми механизмами или поведением принципала, обменивающегося информацией или участвующего в совместной деятельности. Спецификация представлена полностью на метауровне. Разные словари данных, а также инструментальная среда и функциональность гармонизируются посредством метаязыков типа XML Metadata Interchange (XMI) [4].

4 Базовые модели

4.1 Концептуальная структура

Управление полномочиями и авторизация могут быть основаны на ролях, выполняемых отдельными действующими лицами или группами действующих лиц. Действующие лица, взаимодействующие с системными компонентами, называются принципалами. Принципалом может быть пользователь, система, устройство, приложение, компонент или даже объект.

Для построения вышеописанной структуры и функциональности необходим ряд моделей, механизмов, процессов, объектов и т. д., которые должны быть рассмотрены.

Что касается управления полномочиями и контроля доступа, то необходимо рассмотреть два типа базовых классов:

- объекты, к которым относятся документы, принципалы, политики и роли;
- действия, к которым относятся управление политиками, управление принципалами, управление полномочиями, аутентификация, авторизация, управление контролем доступа и аудит.

Следующие модели будут рассмотрены более подробно:

- модель зоны;
- модель документа;
- модель политики;
- модель роли;
- модель авторизации;
- модель управления;
- модель делегирования;
- модель контроля доступа.

Все спецификации данной концептуальной структуры будут открытыми, платформенно независимыми, переносимыми и масштабируемыми. Поэтому предложенные модели описываются на уровнях метамоделей и моделей, а уровень экземпляров не рассматривается. Для такого способа представления систем использованы специфичные языки и метаязыки, например UML и XML, а также средства переноса из одного словаря в другой.

В данной спецификации использованы конструкции UML, спецификации UML, профили UML и всевозможные диаграммы. Что касается XML, то используется несколько спецификаций из стандартного набора XML.

Все используемые модели задают специфические виды ограничений, формирующие модели ограничений. Они охватывают все возможные сервисы или точки зрения на системы. Модель является упрощенным отражением реальности согласно определенным концепциям. Графические модели представлены на языках UML и MOF. Для вербальных моделей использован стандартный набор языка XML.

Предполагается, что многие документы будут представлены на языке XML. Структура подобного документа задается с помощью определения типа документа (DTD) или экземпляра XML-схемы. Политика полномочий может оперировать непосредственно элементами XML (например, сравнивая атрибуты сертификата авторизации с элементами документа).

4.2 Модель зоны

Чтобы информационные системы, обеспечивающие совместный доступ к медицинским данным, были управляемыми и работоспособными, компоненты системы, непосредственно связанные с принципалами, группируются в зоны по принципу общности организационных, логических и технических свойств. Согласно определению OMG (группы управления объектами), такая группировка может быть применена к общим политикам (зоны политик), к общим внешним условиям (зоны внешних условий) или к общим технологиям (зоны технологий). Функциональная совместимость любого вида в пределах зоны называется внутризональным взаимодействием и кооперацией, в то время как функциональная совместимость между зонами называется межзональным взаимодействием и кооперацией. Например, взаимодействие может осуществляться между отделениями больницы внутри больничной зоны (внутризональное взаимодействие), но быть внешним по отношению к зоне конкретного отделения (межзональное взаимодействие). В части требований к информационной безопасности особый интерес представляют зоны политик безопасности.

Зона характеризуется идентификатором зоны, именем зоны, уполномоченным лицом зоны и квалификатором зоны. Предложенное определение типов данных схоже с определением типов данных в HL7, версия 3 [5].

Таблица 1 — Атрибуты зоны политик безопасности

Атрибут	Тип	Примечания
domain_identifier (идентификатор домена)	SET <OID>	Набор (SET) идентификаторов объектов ИСО
domain_name (имя домена)	BAG <EN>	Пакет (BAG) имен сущностей
domain_authority_ID (идентификатор уполномоченного лица зоны)	OID	Идентификатор объекта ИСО
domain_authority_name (имя уполномоченного лица зоны)	ST	Строка
domain_qualifier (квалификатор зоны)	CS	Простое кодированное значение

Класс зоны политик безопасности наследует атрибуты класса зоны и добавляет к ним идентификатор политики и имя политики.

Политика описывает юридически значимую совокупность установленных правил и норм, организационных и административных структур, функциональности, требований и целей, участвующих принципалов, соглашений, прав, обязанностей и штрафных санкций, а также техническое решение, примененное для сбора, регистрации, обработки и передачи данных в информационных системах. Для описания политик могут использоваться такие средства, как шаблоны или формальные модели политик.

В настоящем стандарте зоны определены в общей форме, и на практике их определения могут уточняться. Зона может состоять из субзон (которые наследуют и могут конкретизировать политики родительской зоны). Наименьшей зоной может быть отдельное рабочее место или конкретный компонент информационной системы. Зоны могут объединяться в суперзоны путем связывания отдельных зон и формирования общей зоны большего масштаба для взаимодействия и кооперации.

При межзональном взаимодействии необходимо определить общий набор политик, применяемых ко всем взаимодействующим зонам. Данный набор должен быть определен на основе анализа релевантных политик, специфичных для каждой из взаимодействующих зон. Такие общие политики вырабатываются (согласуются) в процессе, именуемом «наведением мостов» (см. рисунок 2). Уже согласованные политики должны быть документированы и подписаны всеми уполномоченными лицами, отвечающими за обеспечение безопасности в своих зонах (см. ИСО/ТС 22600-1:2006, приложение А). В идеале весь этот процесс должен проводиться с использованием представлений и согласований в электронной форме, чтобы обеспечить взаимодействие в реальном времени в рамках (заранее согласованной) соответствующей и регламентированной структуры. Согласование и верификация политик в этом случае будут иметь место при каждом взаимодействии служб обеспечения безопасности.



Рисунок 2 — Согласование политик

При таком взаимодействии возникает необходимость использования компонентов между принципалами. Концепции промежуточного уровня все чаще используются в архитектуре новых медицинских информационных систем. Промежуточные компоненты могут способствовать обеспечению функциональной совместимости посредством прямого вызова процедуры (коммуникационные сервисы промежуточного уровня) или цепочек вызовов процедур (включая прикладные сервисы промежуточного уровня). В последнем варианте могут использоваться разные модели делегирования (см. 4.8).

Подобная архитектура может быть представлена цепочками, составленными из разных зон, как показано на рисунке 3.



Рисунок 3 — Концепция зон с сервисами промежуточного уровня

С позиций информационной безопасности обычно считается, что зона, обеспечивающая внутризональное взаимодействие в соответствии со своей собственной политикой, нуждается в защите только на границах с внешними зонами с их специфическими политиками (или даже с зоной Интернет без политик). Такая защита осуществляется, например, с помощью межсетевых экранов, прокси-серверов и т. д. Поэтому по отношению к внешнему окружению зона часто считается закрытой. При этом внутренность зоны ошибочно считается безопасной, а внутренние угрозы и вторжения часто игнорируются, в то время как они составляют большинство всех нарушений безопасности.

Учитывая специфические требования и условия здравоохранения, базовая модель информационной безопасности должна учитывать весь спектр сервисов и механизмов обеспечения безопасности, которые могут быть реализованы с помощью защищенных микрозон.

4.3 Модель документа

Процессы, объекты, роли и т. д. должны быть документированы и подписаны, определяя тем самым конкретные отношения между объектами и процессами. Комбинация процессов и отношений приводит к многочисленным подписям на документах (например, при делегировании).

Для обеспечения нескольких подписей на документе в настоящем стандарте используется синтаксис криптографических сообщений. Каждая подпись вычисляется по содержимому документа и факультативно по набору атрибутов, специфичных для конкретной подписи. К таким атрибутам относятся метки времени, назначение подписи и другая информация.

4.4 Модель политики безопасности

Политика безопасности — это комплекс юридических, этических, социальных, организационных, психологических, функциональных и технических положений, призванных обеспечить высокую степень доверия к медицинским информационным системам. В политике формулируются концептуальные требования и условия для достоверного создания, хранения, обработки и использования важной информации.

Политика может быть представлена:

- в вербальной неструктурированной форме;
- в структурированной форме с использованием схем и шаблонов;
- в виде формальной модели.

Для обеспечения функциональной совместимости политика должна быть сформулирована и представлена в виде, обеспечивающем ее правильную интерпретацию и применение на практике. Поэтому на документы, определяющие политику, именуемые также объявлениями политики или соглашениями о политике (соглашения между участвующими партнерами), должны распространяться ограничения на используемые синтаксис, семантику, терминологию и действие.

Чтобы можно было надежно ссылаться на конкретную политику, ее экземпляр должен иметь уникальное имя и идентификатор. То же относится ко всем элементам политики — зоне, целям, действиям и их политикам, которым тоже следует присвоить наименования и уникально идентифицировать. В итоге характеристиками политики безопасности являются идентификатор политики, имя политики, уполномоченное лицо политики, идентификатор зоны, имя зоны, список целей, идентификатор цели, имя цели, объект цели, разрешенные действия и политики, связанные с данной политикой.

Для более наглядного представления в таблице 2 показаны все атрибуты политики, в том числе унаследованные от зоны. Предложенное определение типов данных схоже с определением типов данных в HL7, версия 3 [5].

Медицинские информационные системы, например электронный учет здоровья (ЭУЗ), должны, как минимум, иметь политику безопасности для пациентов, чтобы контролировать доступ к информации об их здоровье, политику с общими правилами доступа для организации, политики, отражающие требования законодательства и других нормативных документов, и по одной политике для каждой структурной роли и каждой функциональной роли.

Каждое создание, доступ или модификация компонента ЭУЗ должно подпадать под действие одной или нескольких политик. Согласно эталонной модели выписки из ЭУЗ, класс его компонента содержит атрибут идентификатора политики, чтобы обеспечить возможность ссылок на такие политики на любом уровне детализации в иерархии ЭУЗ. Политики, применяемые конкретно к ЭУЗ, включая любые связанные с ними политики, могут быть включены в выписку из ЭУЗ.

Как и к любым другим компонентам, к компонентам политики можно применять операции композиции и декомпозиции в соответствии с базовой компонентной моделью. Пользуясь определением типов данных из [5], классы политики могут быть определены как базовая политика, метаполитика и составная политика (см. рисунок 4). Эти классы подробно описаны в таблицах 2, 3 и 4 соответственно, см. [6].

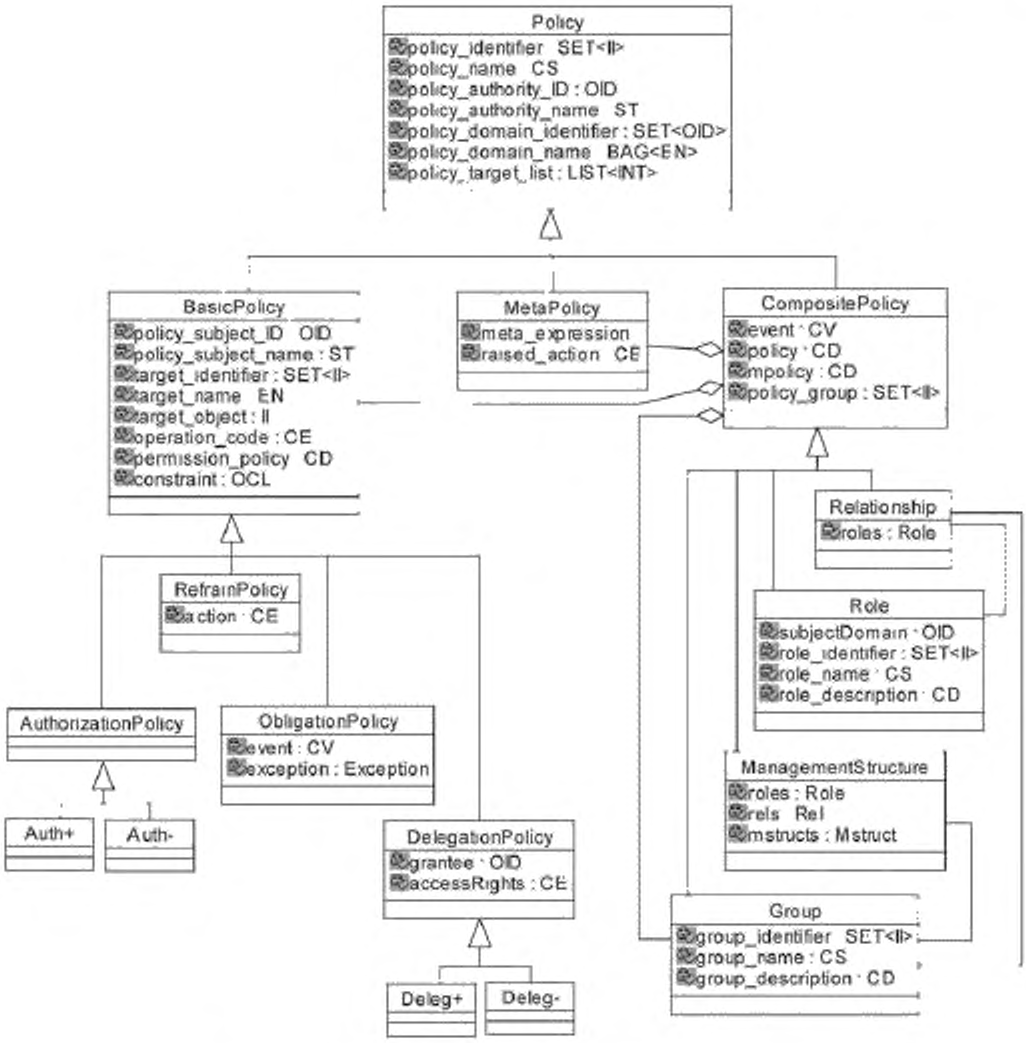

Рисунок 4 — Диаграмма базовых классов политики безопасности

Конкретизации абстрактного класса составной политики сложным образом взаимосвязаны, что обозначено на диаграмме в виде простой ассоциации.

Таблица 2 — Атрибуты базовой политики безопасности

Атрибут	Тип	Примечания
policy_identifier (идентификатор политики)	SET <II>	Набор (SET) идентификаторов экземпляров
policy_name (имя политики)	CS	Простое кодированное значение
policy_authority_ID (идентификатор уполномоченного лица политики)	OID	Идентификатор объекта ИСО

Окончание таблицы 2

Атрибут	Тип	Примечания
policy_authority_name (имя уполномоченного лица политики)	ST	Строка
domain_identifier (идентификатор зоны)	SET <OID>	Набор (SET) идентификаторов объектов ИСО
domain_name (имя зоны)	BAG <EN>	Пакет (BAG) имен сущностей
target_list (список целей)	LIST <INT>	Список элементов типа INT
target_ID (идентификатор цели)	SET <II>	Набор (SET) идентификаторов экземпляров
target_name (имя цели)	EN	Имя сущности
target_object (объект цели)	II	Идентификатор экземпляра
operation_code (код действия)	CE	Кодированный тип данных с возможностью указания эквивалентов
Policies (политики)	CD	Концептуальное описание

Таблица 3 — Типы базовой политики

Тип базовой политики	Назначение	Содержание
Политики авторизации	Определяют разрешенные действия	Субъект (кроме ролей), цель, действие
Политики обязательств	Управляются событиями и определяют действия, выполняемые агентами администратора	Субъект (кроме ролей), действие, событие
Политики воздержания	Определяют действия, от совершения которых субъекты должны воздержаться	Субъект (кроме ролей), действие
Политики делегирования	Определяют, какие полномочия кому могут быть делегированы	—

Таблица 4 — Типы составной политики

Тип составной политики	Назначение
Группы	Определяет область действия связанных политик, к которым может применяться ряд ограничений
Роли	Определяет группу политик (политики авторизации, обязательств и воздержания) (подробнее о ролях см. 4.5 и приложение А)
Взаимосвязи	Определяет группу политик, относящихся к взаимодействиям между ролями

Другой способ декомпозиции политик представлен в спецификации сервисов безопасности, предложенной группой OMG, различающей следующие политики:

- политика доступа вызовов, реализующая политику контроля доступа к объектам;
- политика аудита вызовов, контролирующая тип событий и критерии аудита;
- политика безопасных вызовов, определяющая политики безопасности, связанные с ассоциациями безопасности и защитой сообщений.

В зависимости от требований к разным типам объектов определены.

- политика делегирования вызовов;
- политика доступа приложений;
- политика аудита приложений;
- политика неоспоримости.

Наиболее распространенным способом представления ограничений является спецификация пользовательских схем, например XML-схем. Для обеспечения упомянутой выше функциональной совместимости такая схема должна быть стандартизована.

На рисунке 5 представлен простой пример XML-документа, описывающего политику безопасности.

Политики должны управляться и храниться в стандартизованных надежных репозитариях политик.

```
<policy>
        <policy_name/>
        <policy_identifier/>
        <policy_authority/>
        <domain_name/>
        <domain_identifier/>
        <target_list>
                <target_name/>
                <target_ID/>
                <target_object>
                        <operations/>
                        <policies/>
                </target_object>
        </target_list>
</policy>
```

Рисунок 5 — Пример шаблона политики

4.5 Модель роли

Для управления отношениями между субъектами, участвующими в общей деятельности, необходимо определить две группы ролей: организационные роли на стороне субъекта и функциональные роли на стороне действия.

Для облегчения применения настоящего стандарта функциональные и структурные роли представлены в приложении А.

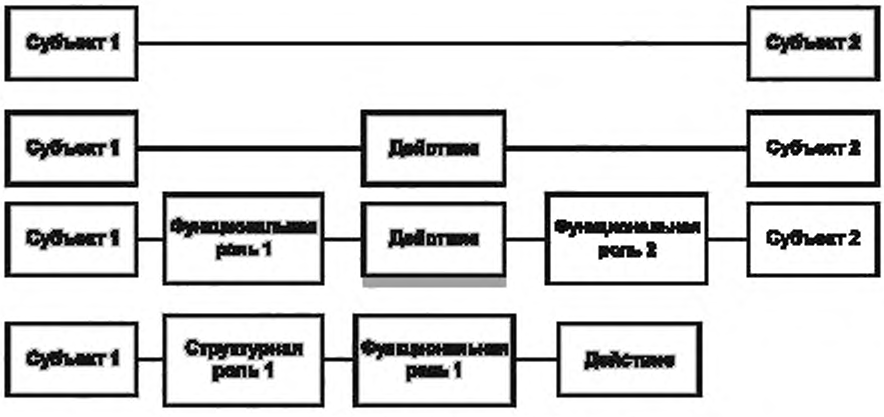

Рисунок 6 — Базовая концепция ролей

4.6 Модель авторизации — назначение ролей и полномочий

Авторизация, проверка свидетельств и полномочий выполняются путем связывания ролей с политиками.

Роли представляют собой средство косвенного назначения полномочий отдельным лицам. Лицам выдаются сертификаты назначения роли, у которых в атрибутах роли указаны одна или несколько ролей. Полномочия назначаются не лицам, а ролям, для чего используются сертификаты спецификации роли. Такое косвенное назначение полномочий позволяет изменять полномочия, назначенные данной роли, не затрагивая сертификаты, назначающие роли отдельным лицам. Сертификаты назначения ролей могут быть сертификатами атрибутов или сертификатами открытого ключа. Сертификаты спецификации ролей не могут быть сертификатами открытого ключа, но должны быть сертификатами атрибутов. Если сертификаты спецификации ролей не используются, то назначение полномочий роли может быть выполнено другими средствами (например, может быть локально сконфигурировано контролером полномочий).

Возможны все следующие сценарии:

- любое число ролей может быть задано уполномоченным лицом по атрибутам (УЛА);
- сама роль и члены роли могут задаваться и администрироваться отдельно, разными УЛА; при этом подразумевается, что роли могут быть локальными в рамках зоны, например на уровне организации, региона или страны;
- членство в роли, как и любое другое полномочие, может делегироваться;
- роли и членству в роли может быть назначен любой требуемый срок действия.

Если сертификат назначения роли является сертификатом атрибута, то атрибут «role» содержится в компоненте «attributes» сертификата атрибута. Если сертификат назначения роли является сертификатом открытого ключа, то атрибут «role» содержится в расширении «subjectDirectoryAttributes». В последнем случае любые дополнительные полномочия, содержащиеся в сертификате открытого ключа, являются полномочиями, непосредственно назначаемыми держателю сертификата. Таким образом, заявитель полномочий может предъявить контролеру полномочий сертификат назначения роли, подтверждающий, что ему назначена данная роль (например, «менеджер» или «покупатель»). Контролер полномочий может знать заранее или установить каким-либо способом, какие полномочия связаны с заявленной ролью, и, соответственно, принять, отклонить или модифицировать запрос на предоставление полномочий. Информацию о полномочиях, назначенных для роли, можно взять из сертификата спецификации роли.

Контролер полномочий должен знать о полномочиях, назначенных роли. Назначение полномочий роли может осуществляться внутри инфраструктуры управления полномочиями (ИУП) посредством сертификата спецификации роли или вне ИУП (например, конфигурируемое локально). Для варианта заявления полномочий в сертификате спецификации роли в настоящем стандарте определены механизмы, позволяющие связать данный сертификат с релевантным сертификатом назначения роли заявителя полномочий. Издатель сертификата назначения роли может отличаться от издателя сертификата спецификации роли, который выдает прилисывающий роль сертификат, и эти сертификаты администрируются (например, создаются, заканчиваются, отзываются) совершенно отдельно. Один и тот же сертификат (сертификат атрибута или сертификат открытого ключа) может содержать сертификат назначения роли, а также прямое назначение лицу других полномочий. Однако сертификат спецификации роли должен быть отдельным сертификатом.

Примечание — Использование ролей в системе авторизации может усложнить процесс обработки пути, поскольку такая функциональность существенным образом задает другой путь делегирования, которому надо следовать. Путь делегирования для сертификата назначения роли может быть связан с разными УЛА и может не зависеть от УЛА, выдавшего сертификат спецификации роли.

Общая модель управления полномочиями описывает три сущности: объект, заявителя полномочий и контролера полномочий. Запрос на предоставление полномочий может быть авторизован, отклонен или модифицирован.

4.7 Модель контроля

Контроль доступа — это процесс определения того, позволяют ли полномочия заявителя получить ему доступ к сервису, предоставляемому целевым компонентом. В данном контексте понятие доступа шире, чем просто получение некоторых данных. Доступ может относиться к любому сервису, предоставляемому целевым компонентом (например, удаление данных, выполнение вычислений, передача информации).

Модель контроля иллюстрирует, каким образом осуществляется контроль доступа к действию с важным объектом. Модель включает четыре компонента: заявителя, контролера, цель и политику контроля (см. рисунок 7).

Заявитель обладает сертификатом атрибутов, содержащим атрибуты полномочий. У цели есть атрибуты важности, которые могут содержаться в грифе секретности, сертификате атрибутов или в локальной базе данных. Описанный здесь метод позволяет контролеру, который может быть владельцем цели или независимым уполномоченным лицом, осуществлять контроль доступа заявителя к цели в соответствии с политикой контроля, а в ряде случаев — с учетом переменных или компонентов среды (например, местного времени).



Рисунок 7 — Модель контроля

Полномочия заявителя обычно инкапсулированы в его сертификате атрибутов. Сертификат атрибутов может быть предъявлен контролеру при запросе услуги (активная стратегия), или передан посредством каких-либо других средств, например через каталог (пассивная стратегия). Необходимо обеспечивать целостность и аутентичность политики контроля, и для этой цели она иногда может фиксироваться вместе с полномочиями заявителя в сертификате атрибутов. Однако обычно политика контроля объявляется отдельно.

Заявитель может быть объектом, идентифицируемым посредством сертификата открытого ключа, либо исполняемым объектом, идентифицируемым посредством справочника.

4.8 Модель делегирования

Кроме модели контроля, нужна еще модель делегирования. В этой модели три компонента: контролер, поставщик полномочий и заявитель (см. рисунок 8).



Рисунок 8 — Модель делегирования

Контролер наделяет объект, известный как поставщик полномочий, глобальным полномочием, распространяющимся на делегирование. Поставщик полномочий является уполномоченным лицом по атрибутам. Он делегирует полномочия заявителям путем выдачи сертификатов атрибутов. Заявитель предъявляет делегированное ему полномочие, демонстрируя свою подлинность. Это может быть сделано путем доказательства обладания секретным ключом, открытая часть которого содержится в сертификате открытого ключа, на который ссылается сертификат атрибутов, содержащий заявленное полномочие.

В некоторых случаях один заявитель может делегировать свое полномочие другому заявителю. Контролер должен подтвердить, что все объекты на пути делегирования обладают достаточными полномочиями для доступа к цели, затребованной непосредственным заявителем.

Поставщик полномочий может также отреагировать на запрос объекта на делегирование его полномочий выдачей сертификата атрибутов другому объекту. Однако описание этого процесса выходит за область применения настоящего стандарта.

Заявитель и контролер могут быть объектами из разных зон безопасности. В этом случае поставщик полномочий может располагаться в зоне контролера, а непрерывная часть пути делегирования, включающая непосредственного заявителя, должна находиться в другой зоне безопасности.

Путь делегирования отличается от пути проверки достоверности сертификатов, используемого для удостоверения подлинности сертификатов открытого ключа объектов, вовлеченных в процесс делегирования. Однако качество аутентичности, обеспечиваемое процессом удостоверения подлинности сертификата открытого ключа, должно быть соразмерно с важностью защищаемой цели.

Определяя функциональную совместимость между распределенными объектами или компонентами, группа управления объектами (OMG) создала альтернативную модель делегирования в рамках своей спецификации сервисов безопасности CORBA. В объектной системе клиент вызывает объект для выполнения некоторого действия, но этот объект нередко не может выполнить это действие сам и вызывает для этого другие объекты. Результатом этого обычно является цепочка вызовов других объектов (более подробно см. на сайте www.omg.org).

При делегировании полномочий информация о правах доступа принципала (т. е. атрибуты безопасности), инициировавшего запрос, может быть делегирована другим объектам в цепочке, чтобы при определенных обстоятельствах ее получатель имел право действовать от имени этого принципала.

Другая схема авторизации использует ссылочное делегирование, при котором права на использование объекта при заданных условиях передаются получателю как часть ссылки на объект. Ссылочное делегирование не рассматривается в настоящем стандарте.

При описании возможностей делегирования, предложенных группой по управлению объектами (OMG), применяют следующие термины:

- **инициатор** (initiator): Первый клиент в цепочке вызовов.
- **конечная цель** (final target): Конечный получатель в цепочке вызовов.
- **посредник** (intermediate): Объект в цепочке вызовов, который не является ни инициатором, ни конечной целью.
- **непосредственно вызывающий** (immediate invoker): Объект или клиент, от которого объект получает вызов.

Обмен медицинской информацией нередко связан с цепочкой поставщиков, реализующих этот обмен (в котором, например, участвуют секретари, медрегистраторы, вспомогательные отделения, а также любые другие принципалы). Данная модель делегирования должна использоваться для любой такой цепочки услуг. См. таблицу 5.

4.9 Модель контроля доступа

Использование ролей может значительно упростить администрирование информационной безопасности. Кроме того, может потребоваться введение административных ограничений. Например, достаточно широко используется ограничение авторизации по принципу разделения обязанностей.

Базовыми элементами управления контролем доступа являются принципалы, роли, разрешения, операции и объекты. Управление контролем доступа включает в себя следующие аспекты:

- определение ролей и ограничений ролей;
- назначение роли пользователю;
- назначение разрешений роли;
- задание ограничений для активизации ролей, назначенных пользователю.

Таблица 5 — Схемы делегирования (по OMG)

Выполняются посредником	Цель	Ограничения
1 Один метод на один объект 2 Несколько методов на один объект		
3 Любой метод на:	а) один объект	Нет
	b) некоторые объекты	Ограничения цели
	c) любой объект	Нет ограничений цели
	без использования полномочий подмножество полномочий инициатора	Простое делегирование
	с использованием полномочий как инициатора, так и своих собственных	Составное делегирование
	полученные полномочия и свои собственные полномочия	Объединенное или отслеживаемое делегирование в зависимости от того, объединяются полномочия или связываются в цепочку
	в течение некоторого срока действия	Ограничения по времени
	для заданного числа вызовов	Ограничения по времени

На основе гармонизации моделей ролей, определенных в 4.5 и приложении А, и усовершенствованных моделей контроля доступа, например стандартного ролевого управления доступом Национального института стандартов США, была разработана адаптированная схема ролевого контроля доступа, представленная на рисунке 9.

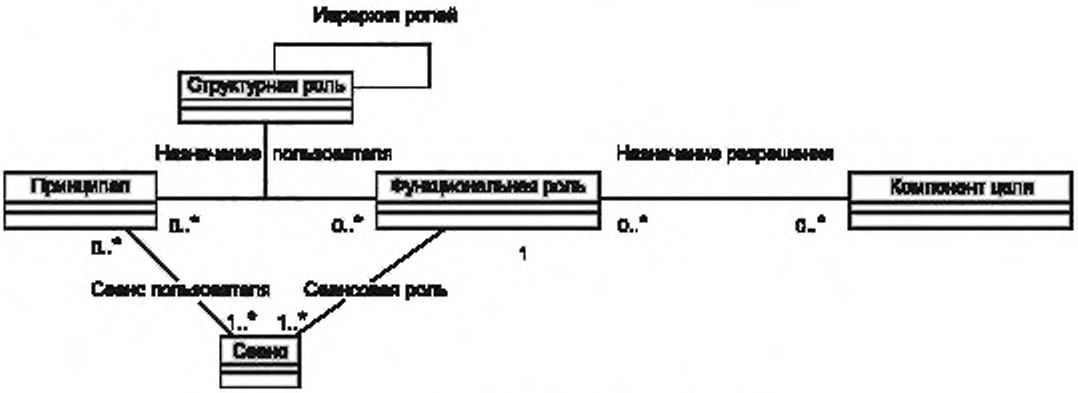

Рисунок 9 — Схема ролевого контроля доступа

Согласно схеме ролевого контроля доступа (РКД) разрешения доступа присваиваются функциональной роли, которая назначается принципалу на время конкретного сеанса доступа. Функциональная роль может быть определена набором структурных ролей, назначенных тому же самому принципалу.

Каждый из компонентов модели определяется следующими составляющими:

- множеством наборов базовых элементов;
- множеством отношений РКД, связывающих эти наборы элементов (содержащим подмножества декартовых произведений, соответствующие допустимым назначениям);
- множеством функций отображения, которые возвращают экземпляры членов одного набора элементов в зависимости от заданного экземпляра из другого набора элементов.

Приложение А
(справочное)

Функциональные и структурные роли

А.1 Роли, связанные с оказанием медицинской помощи

Для управления отношениями между субъектами роли могут быть назначены любому принципалу. Принципалы являются действующими лицами в здравоохранении, поэтому роли связаны с действующими лицами и действиями.

В общем случае выделяются два типа ролей: структурные и функциональные. Структурные роли отражают структурные аспекты отношений между субъектами. Структурные роли описывают предпосылки, способности и компетенции, необходимые для выполнения действий. Функциональные роли отражают функциональные аспекты взаимоотношений между субъектами. Функциональные роли связаны с реализацией/выполнением действий.

Если рассматривать структурные и функциональные роли в одном контексте, то структурные роли обеспечивают предпосылки/компетенции, которыми должны обладать субъекты для выполнения взаимодействий (действия) в рамках их определенных функциональных ролей. Квалификация, навыки и т. п. влияют как на назначение структурных ролей, так и на выполнение действий в соответствии с их функциональными ролями (рисунок А.1).

Примерами структурных ролей медицинских работников могут служить:

- начальник медицинской службы;
- заведующий клиникой;
- заведующий отделением;
- главный врач;
- ординатор;
- врач;
- интерн;
- стажер;
- главная медсестра;
- медсестра;
- студент-медик.

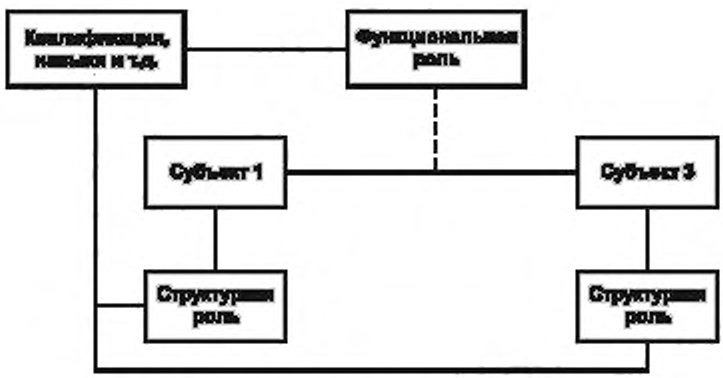

Рисунок А.1 — Общая концепция ролей

Примерами функциональных ролей медицинских работников могут служить:

- лечащий врач;
- сотрудник диагностического отделения;
- сотрудник терапевтического отделения;
- консультант;
- принимающий врач;
- семейный врач;
- операционная медсестра.

А.2 Модель функциональной роли

Применительно к бизнес-процессу оказания медицинской помощи, функциональные роли могут быть определены в терминах уровней авторизации и прав доступа следующим общим способом, опирающимся на частично модифицированные определения, предложенные в австралийском проекте HealthNet, в котором есть ссылки и на другие работы:

- субъект медицинской помощи (обычно пациент);
- агент субъекта медицинской помощи (родитель, опекун, смотритель или другой официальный представитель);
- ответственный (лично) медицинский работник (медицинский работник, находящийся в наиболее тесном контакте с пациентом, нередко его участковый врач);
- полномочный медицинский работник:
- выбранный субъектом медицинской помощи;
- назначенный медицинским учреждением, оказывающим помощь (в соответствии с установленным порядком, практикой и т. д.);
- медицинский работник (непосредственно оказывающий пациенту медицинскую помощь);
- специалист смежной профессии (косвенно участвующий в оказании медицинской помощи, инструктор, исследователь и т. д.);
- администратор (и все остальные участники, обеспечивающие процесс оказания пациенту медицинской помощи).

Данный список фиксирует набор функциональных ролей, предназначенных для управления созданием, доступом, обработкой и обменом медицинской информацией.

Кроме того, функциональные роли могут быть сгруппированы в соответствии с их участием в создании, регистрации, вводе, обработке, хранении и передаче информации:

- составитель информации;
- лицо, подтверждающее информацию;
- лицо, сертифицирующее информацию;
- лицо, авторизующее доступ;
- субъект информации;
- поставщик информации.

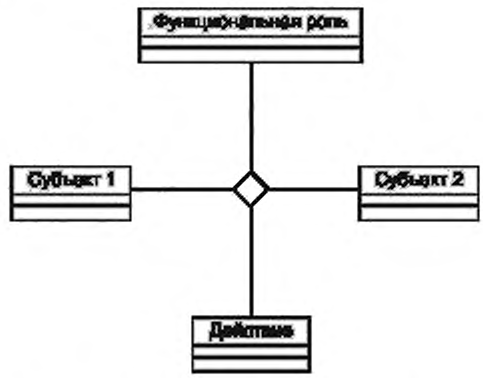

Рисунок А.2 — Модель функциональной роли

Отношения типа «многие ко многим» между субъектами и действиями, преобразованные в соответствии с нотацией UML, представлены на рисунке А.3.

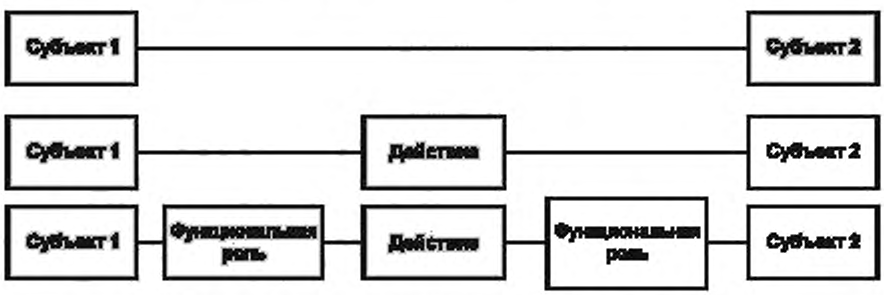

Рисунок А.3 — Развитие модели функциональной роли

А.3 Модель структурной роли

Взаимосвязь типа «субъект — субъект» может затрагивать подрядные действия, результатом которых является заключение контракта между субъектами, исполняющими определенные функциональные роли (см. ниже). Контракт может определять структурную роль личности, например главный врач. Другим примером взаимосвязи «субъект — субъект» является обучение, результатом которого является определенная квалификация, а также сертификат, подтверждающий квалификацию, относящуюся к структурной роли.

Эти уточнения структурных ролей порождают другие взаимосвязи типа «субъект — субъект», влияющие на функциональную роль, исполняемую субъектами, участвующими в данной деятельности. Реализация структурной роли обеспечивается в рамках действия, происходящего между субъектами в соответствии с конкретными функциональными ролями, связанными с данным действием, как показано на рисунке А.4.

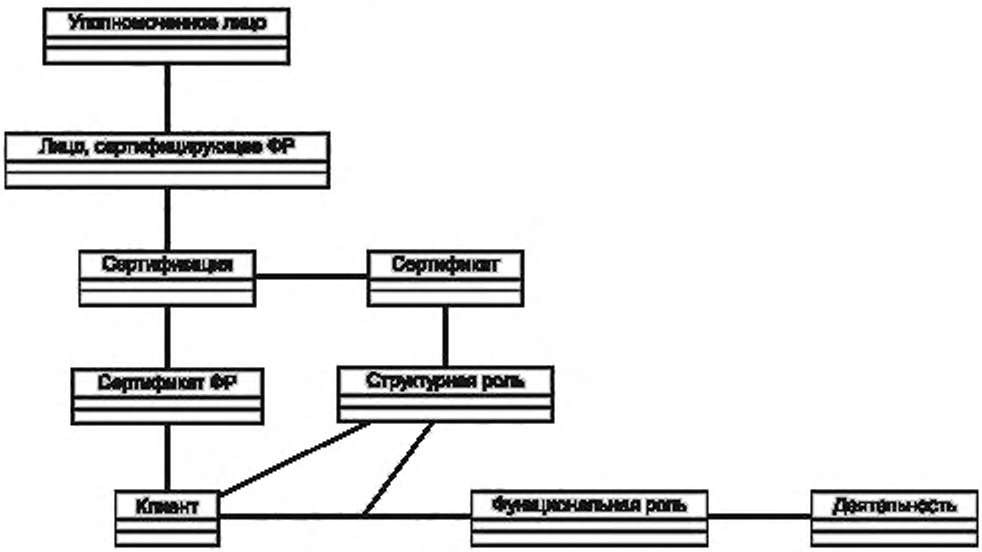

Рисунок А.4 — Реализация структурной роли в деятельности согласно функциональной роли

Если рассматривать структурные и функциональные роли в одном контексте, то структурные роли обеспечивают предпосылки/компетенции, которыми должны обладать субъекты для выполнения взаимодействий (действия) в рамках их определенных функциональных ролей. Квалификация, навыки и т. п. влияют как на назначение структурных ролей, так и на выполнение действий в соответствии с их функциональными ролями.

А.4 Общая спецификация ролей

Класс роли имеет атрибуты, приведенные в таблице А.1.

Таблица А.1 — Атрибуты роли

Атрибут	Тип	Примечания
role_identifier (идентификатор роли)	SET <II>	Множество идентификаторов экземпляров
role_name (имя роли)	CS	Простое кодированное значение
role_authority_ID (идентификатор уполномоченного лица роли)	OID	Идентификатор объекта ИСО
role_authority_ name (имя уполномоченного лица роли)	ST	Строка
role_description (описание роли)	CD	Концептуальное описание

Кроме того, может потребоваться введение административных ограничений. Например, достаточно широко используется ограничение авторизации по принципу разделения обязанностей.

На рисунке А.5 показано описание роли на языке XML.

```
<security_role>
        < role_name/>
        < role_ID/>
        < role_authority_ID/>
        < role_authority_name/>
        < role_description/>
                ...
        < /role_description>
</security_role >
```

Рисунок А.5 — Спецификация роли

Приложение В
(справочное)

Примеры структурных ролей в здравоохранении

Таблица В.1 — Лицензированный медицинский персонал, имеющий разные уровни прав доступа (согласно ASTM E-1986)

Текущий стандартный список лицензированных медицинских работников	Рекомендуемый расширенный список лицензированных медицинских работников
Врач (доктор медицины/аллопат, остеопат, хиропрактик, натуропат, гомеопат)	Врач (с подкатегориями): Хиропрактик Гомеопат Доктор медицины/аллопат Натуропат Остеопат Патолог (новая рекомендованная роль) Психиатр (новая рекомендованная роль) Рентгенолог (новая рекомендованная роль)
Ассистент врача (PA)	Ассистент врача (AB)
Старшая дипломированная медсестра (NP, NM, CAN, CNS)	Медсестра (с подкатегориями): Медсестра-специалист в клинике (МСК) (ранее CNS) Дипломированная медсестра-анестезиолог в клинике (ДМАК) (ранее CAN) Лицензированная медсестра-специалист (ЛМС)/лицензированная медсестра-практик (ЛМП) [ранее «лицензированная медсестра-специалист» (LVN)] Медсестра-акушерка (МА) (ранее «акушерка» и NM) Медсестра-практик (МП) (ранее NP) Дипломированная медсестра (ДМ)
Акушерки	См. Медсестра
Дипломированная медсестра (RN)	См. Медсестра
Лицензированная медсестра-специалист (LVN)	См. Медсестра
Фармацевт (DP)	Фармацевт (с подкатегориями): Фармацевт-аптекарь (новая рекомендованная роль) Фармацевт в клинике (новая рекомендованная роль)
Специалисты нетрадиционной медицины	Специалисты нетрадиционной медицины (с подкатегориями): Иглотерапевт (новая рекомендованная роль) Массажист-терапевт (новая рекомендованная роль)
Поставщики дополнительных медицинских услуг	Рекомендовано упразднить «Поставщики дополнительных медицинских услуг» и заменить на более узкоспециализированные роли поставщиков: Аудиолог (новая рекомендованная роль) Стоматолог (новая рекомендованная роль) Диетолог (новая рекомендованная роль) Психолог (новая рекомендованная роль) Специалист по патологии речи (новая рекомендованная роль) Ветеринар (новая рекомендованная роль)

Окончание таблицы В.1

Текущий стандартный список лицензированных медицинских работников	Рекомендуемый расширенный список лицензированных медицинских работников
Трудотерапия	Терапевт (с подкатегориями): Аудиотерапевт (новая рекомендованная роль) Терапевт-инструктор (новая рекомендованная роль) Кинезиотерапевт (новая рекомендованная роль) Музыкальный терапевт (новая рекомендованная роль) Трудотерапевт (ранее «Трудотерапия») Физиотерапевт (ранее «Физиотерапия») Терапевт по отдыху и оздоровлению (новая рекомендованная роль) Специалист по дыхательной терапии (ранее «Дыхательная терапия») Логопед (ранее «Логопедия») Терапевт по профориентации инвалидов (новая рекомендованная роль)
Физиотерапия	См. Терапевт
Логопедия	См. Терапевт
Дыхательная терапия	См. Терапевт
Лаборант	Лаборант (с подкатегориями): Лаборант отделения кардиологии (новая рекомендованная роль) Лаборант в лаборатории (новая рекомендованная роль) Лаборант-фармаколог (новая рекомендованная роль) Лаборант-протезист Лаборант-рентгенолог (новая рекомендованная роль)
Техник по наложению шин и гипса	Рекомендовано упразднить. См. Лаборант
Техник-протезист	См. Лаборант
(Отсутствует)	Технолог (с подкатегориями) (новая рекомендованная роль) Лаборант-технолог (новая рекомендованная роль)

Библиография

[1] Blobel, B., Assessment of Middleware Concepts Using a Generic Component Model, Proceedings of the Conference «Toward An Electronic Health Record Europe '97», pp. 221—228. 20—23 October 1997, London

[2] Blobel, B., Application of the Component Paradigm for Analysis and Design of Advanced Health System Architectures. International Journal of Medical Informatics 60 (3), pp. 281—301, 2000

[3] Blobel, B., Analysis, Design and Implementation of Secure and Interoperable Distributed Health Information Systems, Series «Studies in Health Technology and Informatics» 89, IOS Press, Amsterdam, 2002

[4] World Wide Web Consortium: Metadata Interchange Format (XMI): gost.e-ecolog.ru

[5] Health Level Seven, Inc.: gost.e-ecolog.ru

[6] Damianou, N., Dulay, N., Lupu, E. and Sloman, M., Ponder: A Language for Specifying Security and Management Policies for Distributed Systems, The Language Specification, Version 2.3. Imperial College Research Report DoC 2000/1. 20 October, 2000

[7] ISO/IEC 2382-8:1998, Information technology — Vocabulary — Part 8: Security

[8] ISO 7498-2:1989, Information processing systems — Open Systems Interconnection — Basic Reference Model — Part 2: Security Architecture

[9] ISO/IEC 8824-1:2002, Information technology — Abstract Syntax Notation One (ASN.1): Specification of basic notation — Part 1
[10] ISO/IEC 9594-8:2001, Information technology — Open Systems Interconnection — The Directory: Public-key and attribute certificate frameworks — Part 8
[11] ISO/IEC 9798-3:1998, Information technology — Security techniques — Entity authentication — Part 3: Mechanisms using digital signature techniques
[12] ISO/IEC 10181-1:1996, Information technology — Open Systems Interconnection — Security frameworks for open systems: Overview
[13] ISO/IEC TR 13335-1:2004, Information technology — Security techniques — Management of information and communications technology security — Part 1: Concepts and models for information and communications technology security management
[14] ISO/IEC TR 14516:2002, Information technology — Security techniques — Guidelines for the use and management of Trusted Third Party services
[15] ISO/IEC 15945:2002, Information technology — Security techniques — Specification of TTP services to support the application of digital signatures
[16] ISO/IEC 17799:2005, Information technology — Security techniques — Code of practice for information security management
[17] ENV 13729:2000, Health informatics — Secure user identification — Strong authentication using microprocessor cards
[18] ENV 13608-1:2000, Health informatics — Security for healthcare communication — Part 1: Concepts and terminology
[19] ENV 13606-3:2000, Health informatics — Electronic healthcare record communication — Part 3: Distribution rules
[20] ISO/IEC 10746-1, Information technology — Open Distributed Processing — Reference model: Overview
[21] ISO/TS 21298, Health informatics — Functional and structural roles

УДК 004.61:006.354 ОКС 35.240.80 П85 ОКСТУ 4002

Ключевые слова: здравоохранение, информатизация здоровья, управление полномочиями, контроль доступа, формальные модели

Редактор *О. А. Стояновская*
Технический редактор *Н. С. Гришанова*
Корректор *Н. И. Гаврищук*
Компьютерная верстка *В. Н. Романовой*

Сдано в набор 20.08.2010. Подписано в печать 09.09.2010. Формат 60×84 1/8. Бумага офсетная. Гарнитура Ариал. Печать офсетная Усл. печ. л. 3,26. Уч.-изд. л. 2,90. Тираж 89 экз. Зак. 1240.

ФГУП «СТАНДАРТИНФОРМ», 123995 Москва, Гранатный пер., 4.
Набрано и отпечатано в Калужской типографии стандартов, 248021 Калуга, ул. Московская, 256.

gost.e-ecolog.ru gost.e-ecolog.ru gost.e-ecolog.ru