ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 54472— 2011/ ISO/TS 13606-4:2009

Информатизация здоровья

ПЕРЕДАЧА ЭЛЕКТРОННЫХ МЕДИЦИНСКИХ КАРТ

Часть 4

Безопасность

ISO/TS 13606-4:2009
Health informatics — Electronic health record communication — Part 4: Security
(IDT)

Издание официальное

Москва
Стандартинформ
2013

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 бюджетным учреждением «Центральный научно-исследовательский институт организации и информатизации здравоохранения Минздравсоцразвития» (ЦНИИОИЗ Минздравсоцразвития) и Обществом с ограниченной ответственностью «Корпоративные электронные системы» на основе собственного аутентичного перевода на русский язык международного документа, указанного в пункте 4

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

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 18 октября 2011 г. № 467-ст

4 Настоящий стандарт идентичен международному документу ИСО/ТС 13606-4:2009 «Информатизация здоровья. Передача электронных медицинских карт. Часть 4. Безопасность» (ISO/TS 13606-4:2009 «Health informatics — Electronic health record communication — Part 4: Security»)

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

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, 2013

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 Соответствие 1
3 Термины и определения 2
4 Обозначения и сокращения 3
5 Чувствительность компонентов ЭМК и функциональные роли 4
5.1 Чувствительность элемента RECORD_COMPONENT. 4
5.2 Функциональные роли 4
5.3 Отображение функциональной роли на категорию чувствительности элемента RECORD_COMPONENT 5
6 Представление информации о политике доступа в выписке EHR_EXTRACT 6
6.1 Общие положения 6
6.2 Архетип композиции политики доступа. 7
6.3 Представление композиции COMPOSITION архетипа политики доступа на языке ADL 9
6.4 Представление архетипа композиции политики доступа на языке UML 15
7 Представление информации журнала аудита — модель объекта EHR_AUDIT_LOG_EXTRACT . . . 16
Приложение А (справочное) Пример контроля доступа. 19
Приложение В (справочное) Связь со стандартом ENV 13606-3:2000 23
Приложение ДА (справочное) Сведения о соответствии ссылочных международных стандартов и документов ссылочным национальным стандартам Российской Федерации. 30
Библиография 31

Введение

1 Сложность предмета настоящего стандарта

Безопасная передача электронных медицинских карт (ЭМК) целиком или отдельными частями, внутри организации и между организациями, а иногда и между разными странами представляет определенную сложность. Медицинские карты должны создаваться, обрабатываться и управляться таким образом, чтобы была обеспечена конфиденциальность их содержания и чтобы пациенты могли контролировать ее использование в рамках действующего законодательства. Во всем мире эти принципы воплощаются в форме национальных законов о защите персональной информации. Эти законы декларируют, что только субъект медицинской помощи имеет право на принятие решений, связанных с доступом к содержанию и с передачей его медицинской карты. Передача третьей стороне информации, содержащейся в медицинской карте, может иметь место только с согласия пациента в форме подписи, например, согласие на обработку его персональных данных. Для определения соответствующих спецификаций политики безопасности при трансграничной передаче ЭМК могут использоваться методические указания, изложенные в ИСО 22857.

В идеале каждый отдельный элемент медицинской карты пациента должен быть доступен только лицам, имеющим право видеть эту информацию, по выбору или с согласия пациента. Круг лиц, на которые законом возложена обязанность оказания медицинской помощи, динамически меняется на протяжении жизни пациента. Разрешение доступа к этим элементам должно быть также дано тем лицам, которые имеют на это право по причинам, не связанным с непосредственным оказанием медицинской помощи (например, для управления здравоохранением, ответственного за эпидемиологию согласованных исследований общественного здоровья). Однако это не относится к тем данным, которые пациент считает слишком личными. С другой стороны, если пациент или его представители категорируют информацию как персональную или личную, то это не должно препятствовать оказанию экстренной медицинской помощи или вводить в заблуждение медицинских специалистов, которые из-за отсутствия необходимой информации могут принять неправильное решение о лечении пациента. Со временем представление пациента о чувствительности[1)] сведений его медицинской карты может изменяться по мере того, как у него появляется все больше опасений за свое здоровье или меняется отношение общества к проблеме здоровья. Пациенты могут пожелать предоставить гетерогенные права доступа членам семьи, друзьям, лицам, осуществляющим уход, членам своей общины. Члены одной семьи могут пожелать иметь возможность доступа (хотя и не обязательно равного) к медицинским картам друг друга, чтобы следить за изменением состояния здоровья фамильного древа.

Требования к разрешению доступа к ЭМК, бесспорно, намного сложнее, чем те, что практикуются в большинстве других отраслей. Ситуация еще более осложняется следующими причинами:

- большим числом записей в медицинскую карту пациента, обусловленным современными технологиями медицинской помощи;
- значительным числом медицинских работников, часто меняющих свои посты, которые потенциально могут контактировать с пациентом в любой момент времени;
- большим числом организаций здравоохранения, в которые пациент может обращаться на протяжении своей жизни;
- трудностями (как для пациента, так и для других лиц) стандартизованной классификации категорий конфиденциальности элементов медицинской карты;
- трудностями определения, в какой мере и какому именно кругу лиц может понадобиться отдельно взятый элемент ЭМК при будущем оказании медицинской помощи;
- логически преемственной природой ЭМК и необходимостью точного управления изменениями в разрешениях доступа по мере изменения самих элементов ЭМК;
- необходимостью очень быстрого принятия решения о доступе в реальном времени и потенциально в распределенной вычислительной среде;
- большой озабоченностью растущего числа пациентов тем, чтобы их согласие на доступ к данным регистрировалось и соблюдалось;
- известным равнодушием большинства пациентов к этим вопросам, из-за чего данный процесс ранее имел низкий приоритет и ограниченное финансирование.

[1)] Термин «чувствительность» широко используется в документах по информационной безопасности для большого числа предохранительных и управляющих средств, но в настоящем стандарте он относится только к контролю доступа.

Необходимым условием обеспечения интероперабельности систем ведения ЭМК и четкой передачи данных ЭМК от одного поставщика медицинской помощи к другому является автоматизация процесса определения, разрешено ли данному лицу, запрашивающему содержание ЭМК, его получение. Если такая автоматизация невозможна, то задержки в принятии решения и вытекающие отсюда трудности при обмене медицинскими картами сведут на нет все усилия по достижению интероперабельности данных.

Основные принципы подхода к разработке стандартов в области контроля доступа при передаче ЭМК заключаются в таком сопоставлении характеристик и параметров запроса на предоставление данных с политиками владельцев ЭМК, а также с объявлениями разрешений доступа или согласия на доступ, приложенными к конкретной ЭМК, при котором возможность раскрытия информации становилась бы очевидной и поддавалась автоматической обработке.

На практике активно разрабатываются международные стандарты по спецификации систем контроля доступа и управления привилегиями, которые допускали бы чисто машинное принятие решения. Однако этот вид деятельности зависит от усилий служб здравоохранения по достижению консенсуса в части назначения привилегий доступа своим сотрудникам и выделению спектра категорий чувствительности, которые могут быть предложены пациентам для категорирования элементов данных их электронных медицинских карт. Для этого требуется согласованность способов представления релевантной информации, которая позволит эффективно масштабировать эти представления в момент определения элементов данных (при добавлении этих элементов в ЭМК) и во время доступа к ЭМК (когда она извлекается или запрашивается целиком). Способы представления должны быть достаточно устойчивы в течение всей жизни пациента. Важно иметь в виду, что в обозримом будущем многие страны будут применять разные подходы к обеспечению безопасности передачи ЭМК, включая особенности своего законодательства, поэтому включение в стандарты слишком строгих предписаний в настоящее время невозможно.

Настоящий стандарт не предписывает правила доступа (то есть не указывает, кто и к чему должен иметь доступ и с помощью каких механизмов безопасности), они должны задаваться сообществами пользователей, национальными методическими указаниями и законодательством.

Настоящий стандарт определяет основные рамки для минимальной спецификации политики доступа к ЭМК и концентрирует внимание на общем представлении о передаче более детализированной информации об этой политике. Эти рамки дополняют общую архитектуру, описанную в ИСО 13606-1, и определяют специфичные информационные структуры, которые должны передаваться как часть объекта выписки из электронной медицинской карты (EHR_EXTRACT), определенного в ИСО 13606-1.

Формализм, использованный в настоящем стандарте, включает в себя унифицированный язык моделирования UML (Unified Modelling Language; см. дополнительные сведения на странице http://gost.e-ecolog.ru), а также язык описания архетипов ADL (Archetype Definition Language; см. дополнительные сведения на странице gost.e-ecolog.ru).

Некоторые виды соглашений, необходимых для обеспечения безопасной передачи ЭМК, неизбежно оказываются за рамками настоящего стандарта. Полная защита передачи ЭМК требует учета большого числа аспектов, многие из которых не специфичны для медицинской информации.

Примечание — Настоящий стандарт основан на документе EN 13606-4:2007. Его содержание идентично данному документу, за исключением следующего:

- изложение настоящего введения пересмотрено для отражения всемирной, а не только европейской юрисдикции;
- вместо ссылок на разрабатываемый стандарт безопасности включены ссылки на опубликованный стандарт;
- где это уместно, добавлены ссылки на новые разрабатываемые стандарты безопасности;
- в первой строке в таблице 2 (классификация категорий чувствительности) вместо «персональная медицинская помощь» указано «личные сведения»;
- исправлено небольшое число опечаток и неоднозначностей.

2 Сценарии обмена

2.1 Потоки данных

Модели интерфейсов и сообщений, необходимых для обеспечения передачи ЭМК, рассматриваются в ИСО 13606-5. Приведенная в настоящем стандарте общая схема процесса передачи призвана показать акты взаимодействия, в которых требуется обеспечение безопасности. На рисунке 1 показа-

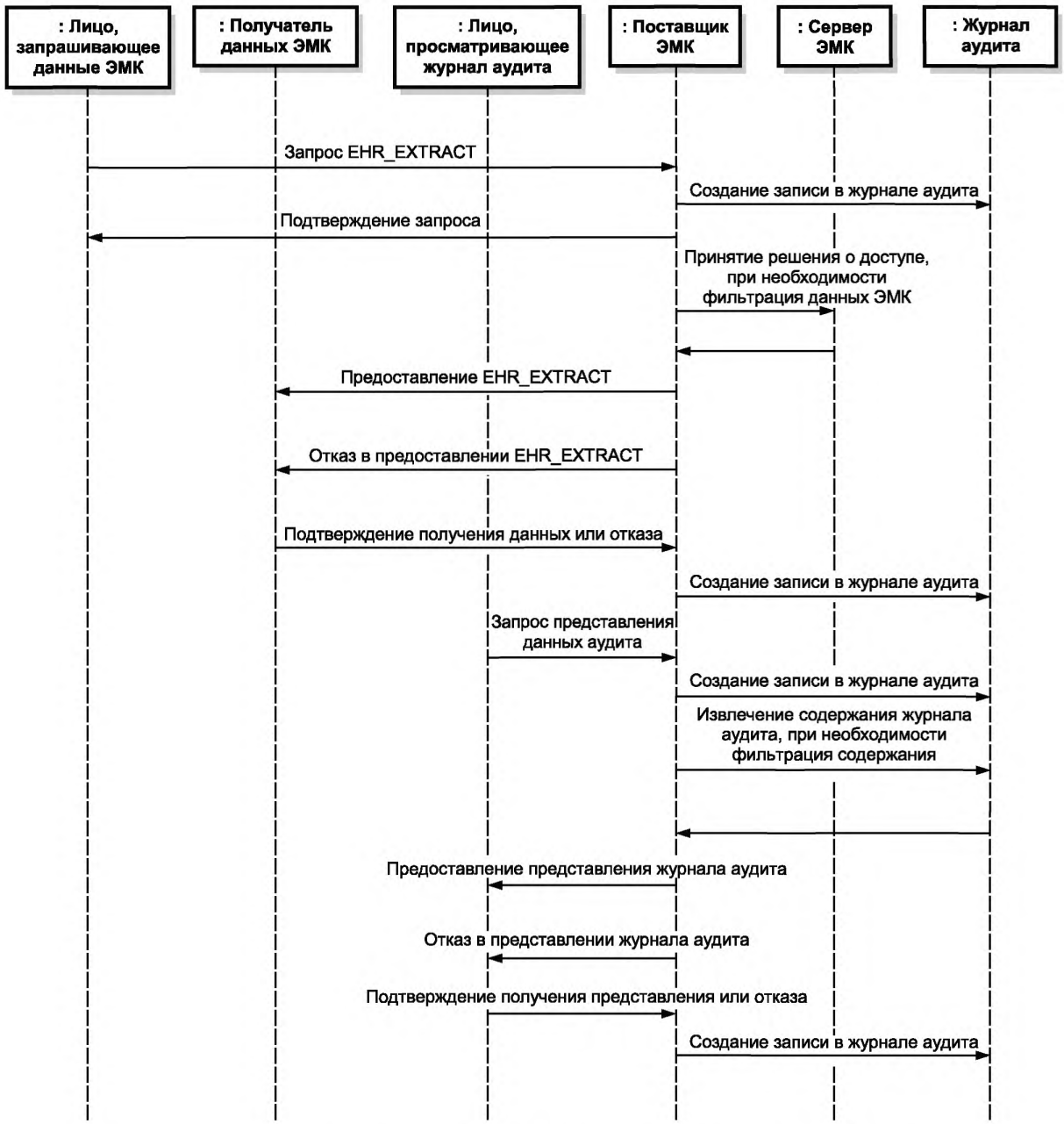


Рисунок 1 — Основные потоки данных и процессы обработки, связанные с обеспечением безопасности, рассматриваемые в настоящем стандарте

ны основные потоки данных и сценарии, которые должны быть рассмотрены в настоящем стандарте. Каждый основной поток должен сопровождаться подтверждающим ответом, и в качестве ответа вместо запрошенных данных может возвращаться сообщение об ошибке.

Лицами, запрашивающими ЭМК, получающими ЭМК и анализирующими журнал доступа, могут быть медицинские специалисты, пациент, его полномочный представитель или другая сторона, наделенная достаточными правами доступа к медицинской информации. Содержание объекта выписки EHR_EXTRACT и журнала доступа, если таковой представляется, может фильтроваться в целях ограничения раскрываемой информации в зависимости от привилегий ее получателя.

Примечание — Журнал доступа должны вести все стороны, участвующие во взаимодействии, а не только поставщик ЭМК. Однако в целях упрощения представления процессы обработки других журналов на схеме не показаны и не описаны.

2.2 Запрос выписки из ЭМК

Запрос выписки требуется не всегда, иногда данные ЭМК могут отправляться получателю без предварительного запроса, как это имеет место в случае выписного эпикриза. Интерфейс запроса должен включать в себя профиль запрашивающего лица, достаточный для того, чтобы поставщик ЭМК мог принять обоснованное решение о доступе, внести необходимые сведения в журнал доступа и предоставить требуемые данные указанному получателю. В некоторых случаях лицо, запрашивающее ЭМК, может отличаться от получателя ЭМК. Например, агентское программное обеспечение может создавать уведомление, содержащее данные ЭМК, и направлять его медицинскому специалисту. В таком случае решение о предоставлении доступа должно приниматься на основании привилегий, которыми наделен получатель ЭМК.

Может требоваться, чтобы запрос ЭМК сопровождался данными информированного согласия на доступ или направления на лечение либо ссылкой на такое согласие или направление, то есть предусматривать некоторую форму явного согласия пациента или направления на лечение.

Достижение договоренности между лицом, запрашивающим данные, и поставщиком данных постепенно будет автоматизироваться, и информация, включаемая в такой запрос, должна быть достаточной для того, чтобы решение о предоставлении доступа принималось автоматически.

Требования к такому взаимодействию отражены в модели интерфейса запроса EHR_Request, включенной в ИСО 13606-5.

2.3 Создание записи в журнале аудита

Практика ведения журнала аудита доступа необходима всем системам ведения ЭМК, но нормативный интерфейс к журналу доступа не специфицируется, поскольку в действующих системах подходы к реализации журнала и предоставляемые возможности существенно различаются. Для интероперабельности наличие подсистемы аудита в системе ведения ЭМК не является необходимым, за исключением ситуации, когда требуется обеспечить реализацию модели, описанной в разделе 7, и соответствующего интерфейса, описанного в ИСО 13606-5.

2.4 Подтверждение получения запроса выписки из ЭМК (EHR_Request)

Что-либо специфичное для здравоохранения не предлагается.

2.5 Принятие решения о доступе, фильтрация данных ЭМК

При обработке запроса на получение данных ЭМК и принятии решения о том, какие данные извлекаются из ЭМК, должны учитываться политики, которыми руководствуется поставщик ЭМК, а также политики доступа, описанные в самой ЭМК. Настоящий стандарт не может указать полный набор политик, которые могут влиять на действия поставщика ЭМК, поскольку они должны регламентироваться национальным и местным законодательством, а также профессиональными, корпоративными и другими правилами.

Решение о фильтрации данных ЭМК на основе категорирования чувствительности ее элементов, учитывающего привилегии, имеющиеся у лица, запрашивающего ЭМК, и лица, получающего ЭМК, должно удовлетворять соответствующим политикам и может потребовать нахождения баланса между клиническими рисками, вызванными отказом в предоставлении данных, и медико-правовыми рисками раскрытия информации.

Настоящий стандарт не определяет весь базис интероперабельного представления политик доступа, которые могут быть наложены на конкретную ЭМК самим пациентом или его представителями. Такие политики могут не храниться в физической системе ведения ЭМК, они могут быть, к примеру, интегрированы в сервер политик доступа, связанный с сервером ЭМК.

Более детально принятие решения о доступе описано в разделе 5.

2.6 Отказ в предоставлении выписки HER_EXTRACT

При принятии решения об отклонении запроса о предоставлении выписки из ЭМК необходимо установить приблизительный перечень причин отказа, по которому будет определена соответствующая

совокупность ответов поставщика ЭМК. Важно иметь в виду, что отказ в доступе, по какой бы причине он не был дан, не должен информировать получателя, что запрошенные им данные ЭМК существуют — одно только раскрытие факта их существования может повредить пациенту.

Причины отказа, специфичные для здравоохранения, не предлагаются; модель интерфейса описана в ИСО 13606-5.

2.7 Предоставление выписки EHR_EXTRACT

Лицо, запрашивающее данные ЭМК, может не совпадать с получателем данных ЭМК, и предоставление этих данных не обязательно инициируется запросом. Предоставление этих данных может происходить по инициативе поставщика ЭМК при оказании этапной медицинской помощи или при добавлении новых данных в ЭМК.

Объект EHR_EXTRACT должен соответствовать эталонной информационной модели, определенной в ИСО 13606-1, и модели интерфейса, определенной в ИСО 13606-5.

В целях управления дальнейшей передачей данных ЭМК объект EHR_EXTRACT должен включать в себя по значению или по ссылке все релевантные политики доступа, представленные в соответствии с данным стандартом. Передача по ссылке может практиковаться только в том случае, если известно, что получатель данных ЭМК имеет прямой доступ к содержанию политик иными средствами.

2.8 Подтверждение получения объекта EHR_EXTRACT

Подтверждения получения объекта EHR_EXTRACT, специфичные для здравоохранения, не предлагаются.

2.9 Создание записи в журнале аудита

См. 2.3.

2.10 Запрос представления данных аудита

В настоящее время желательно, чтобы пациент имел возможность узнать, кто получал доступ к части или ко всей его ЭМК в распределенной вычислительной среде. Согласно определению, данному в настоящем стандарте, назначение такого интерфейса — запросить представление журнала аудита, которое информирует получателя о том, кто и когда имел доступ к данной ЭМК, и к каким ее частям. Он не рассчитан на ситуацию, когда необходим полный просмотр журнала, например при судебном или ином расследовании. Соответствующий интерфейс описан в разделе 5.

Модель интерфейса определена в ИСО 13606-5.

2.11 Создание записи в журнале аудита

См. 2.3.

2.12 Предоставление представления для просмотра журнала доступа к ЭМК

Данная практика требует реализации интероперабельного представления записи журнала (или совокупности записей). Соответствующий интерфейс описан в разделе 5.

Хотя при официальном расследовании требуется, чтобы журнал доступа предоставлялся в полной немодифицированной форме, представление, сконструированное для просмотра журнала пациентом или медицинским специалистом, может включать в себя фильтрацию лишних записей (например, относящихся к данным ЭМК, к которым пациент не имеет доступа).

Модель интерфейса определена в ИСО 13606-5.

2.13 Отказ в представлении журнала аудита

Если запрос на просмотр журнала доступа не удовлетворяется, то надо определить приблизительный перечень причин отказа. Важно иметь в виду, что отказ в просмотре, по какой бы причине он не был дан, не должен информировать получателя, что запрошенные им данные ЭМК существуют — одно только раскрытие факта их существования может повредить пациенту.

Подтверждение причины отказа в представлении журнала аудита, специфичное для здравоохранения, не предлагается; модель интерфейса описана в ИСО 13606-5.

2.14 Подтверждение получения представления журнала аудита

Подтверждение получения представления журнала аудита, специфичное для здравоохранения, не предлагается.

2.15 Создание записи в журнале аудита

См. 2.3.

3 Требования и технический подход

3.1 Исследование требований

Выполненные исследовательские работы, национальные и международные стандарты по интероперабельному обмену электронными медицинскими картами способствуют тому, чтобы разнородные клинические информационные системы могли обмениваться электронными медицинскими картами пациентов или их частями стандартизованным способом, обеспечивающим точное и достаточно общее представление значений данных, контекстуальной организации и медико-правовое происхождение информации, возникающей в какой-либо из систем ведения ЭМК. Чувствительная информация, например, та, что обрабатывается системами ведения ЭМК, должна регистрироваться, храниться и передаваться безопасным, защищенным и надежным способом. Следовательно, передача ЭМК должна удовлетворять требованиям безопасности, примерами которых могут служить:

- аутентификация субъектов (людей, компонентов программного обеспечения, устройств и т. д.), которые на законных основаниях могут запрашивать или представлять данные электронных медицинских карт;
- управление авторизацией, привилегиями и контроль доступа;
- обеспечение целостности хранимой, обрабатываемой и передаваемой информации, содержащейся в ЭМК;
- категорирование информации, содержащейся в ЭМК;
- определение, согласование и отображение политик при взаимодействии субъектов, запрашивающих и предоставляющих данные ЭМК;
- обеспечение отчетности и отслеживания доступа, обработки и передачи информации;
- общие процедуры безопасности и обеспечения качества.

К числу основополагающих научно-исследовательских работ в этой области относятся такие европейские проекты, как SEISMED, TrustHealth и HARP.

Большинство информационных систем организаций здравоохранения уже имеет системы и службы безопасности, предназначенные для защиты широкого спектра данных, связанных со здоровьем. Передача ЭМК служит только одним примером. Кроме того, для обеспечения защиты информации о здоровье активно разрабатываются общие подходы к описанию, реализации, профилированию и оценке постоянно усложняющихся служб безопасности. Многие требования, предъявляемые к передаче ЭМК, равным образом применимы и к общему случаю передачи информации в здравоохранении.

3.2 Общие требования информационной безопасности в здравоохранении

Наиболее широко признанные требования к обеспечению безопасности чувствительных и персональных данных изложены в стандарте ИСО/МЭК 27002. В нем указаны виды мер, которые должны предприниматься для защиты таких активов, как ЭМК, и способы безопасной передачи данных в распределенной вычислительной среде. Руководство по применению этого общего стандарта в информационных системах здравоохранения опубликовано в стандарте ИСО 27799. Его применение упростит формулирование общих политик информационной безопасности для учреждений здравоохранения и будет способствовать распространению интероперабельных компонентов и служб безопасности.

Руководство по обеспечению трансграничной передачи ЭМК содержится в стандарте ИСО 22587. Он может быть использован для разработки соответствующих спецификаций политик безопасности.

Требования по защите, которые должны выполняться каждым конкретным участником обмена ЭМК, будут определяться национальными и местными политиками, обязательными для каждой участвующей стороны, а также для всех промежуточных узлов в цепочке обмена данными. Многие из этих политик распространяются на все обмены данными в здравоохранении, но имеют отличия в зависимости от стран и условий оказания медицинской помощи, поэтому они не регулируются настоящим стандартом.

Любой доступ к данным ЭМК требует, чтобы запрашивающая сторона была соответствующим образом аутентифицирована, чтобы пользователю, программному компоненту или устройству было разрешено делать запрос, и, если это условие выполнено, чтобы поименованному получателю данных ЭМК (который может отличаться от запрашивающего субъекта) было разрешено получить эти данные. Все обмены данными должны осуществляться по защищенным каналам передачи данных, и журнал аудита должен хранить весь «след» движения данных ЭМК. Инфраструктура, обеспечивающая такие службы безопасности, будет общей для многих сфер, а не только для здравоохранения. Разработчики настоящего стандарта предполагают, что эти службы уже имеются и задействованы для всех обменов данными ЭМК. Поэтому они исходили из предположения, что у всех участников обмена данными ЭМК имеются общие политики или набор политик, удовлетворяющих стандарту ИСО 27799, и что эти политики соответствуют национальному законодательству или международным договорам по защите информации. Для удовлетворения специфичных национальных, региональных, профессиональных или ведомственных требований, распространяющихся на передачу или использование данных электронных медицинских карт, могут потребоваться дополнительные политики. Определение таких политик не является целью настоящего стандарта.

3.3 Общая архитектура контроля доступа в информационных системах здравоохранения

Легитимность доступа к данным ЭМК определяется большим числом политик, которые могут существовать в форме документов или программного кода либо быть встроенными в компоненты систем формальной авторизации. Известно, что производители и организации по-разному подходят к реализации политик и сервисов контроля доступа и степень их компьютеризации отличается.

Стандарт ИСО/ТС 22600 определяет общую логическую модель представления привилегий принципалов (субъектов доступа), политик контроля доступа к потенциальным целевым объектам и процесса согласования, требуемого для принятия решения о доступе. В настоящем стандарте дается общий подход к таким задачам, как назначение ролей субъектам и передача ролей от одного субъекта другому.

На рисунке 2 изображены ключевые понятия ролевого контроля доступа согласно определениям ИСО/ТС 22600.

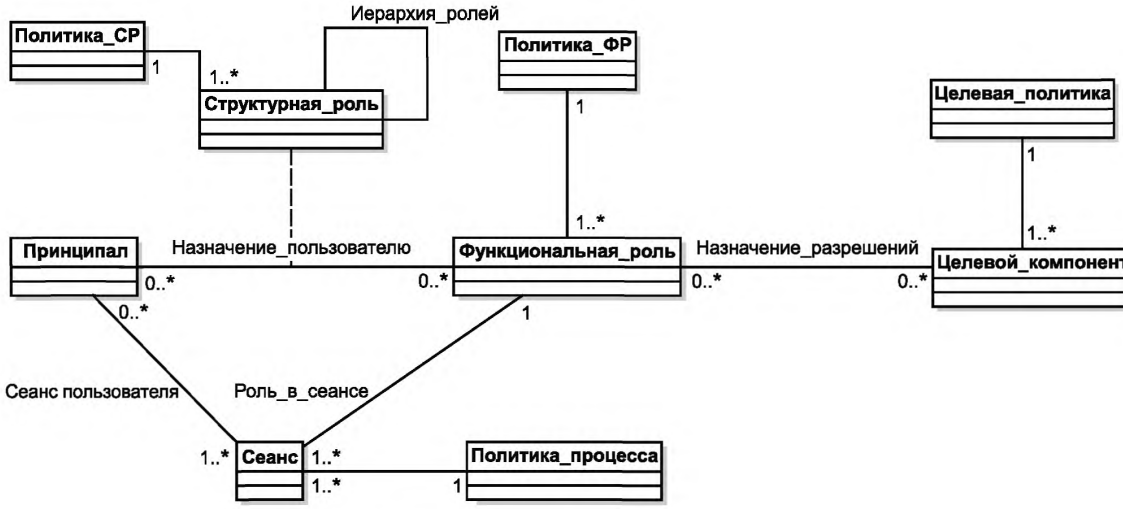


Рисунок 2 — Основные понятия и типы политик, определенные в ролевом контроле доступа

Принципалам (лицам, агентам и т. д.) назначаются структурные роли и в зависимости от них — одна или несколько функциональных ролей. Например, лицо с медицинским образованием и специальностью педиатра может иметь несколько структурных ролей (консультирующий педиатр в больнице, заведующий региональным отделом детского скрининга). Эти структурные роли могут разрешать ему время от времени выполнять функциональную роль лечащего врача пациента. Функциональная роль может быть постоянной или ограниченной одним сеансом доступа. Функциональным ролям назначаются разрешения на выполнение конкретных действий (например, внесение новой записи в ЭМК) с кон-

кретными объектами (например, с данными электронной медицинской карты, которые носитель роли имеет право видеть).

В настоящем стандарте класс целевого компонента (Target_Component), показанный на рисунке 2, трактуется как данные электронной медицинской карты, принадлежащие поставщику ЭМК. Класс целевой политики (Target_Policy) содержит информацию, которая определяет правила разрешения или отказа в доступе ко всей ЭМК или к ее части. Если объект выписки из ЭМК (EHR_EXTRACT) создан и содержит эти данные электронной медицинской карты, то получателю ЭМК должны быть также переданы соответствующие целевые политики. Это требует включения в выписку EHR_EXTRACT интероперабельного представления политики Target_Policy.

Инженерные и технологические реализации этой инфраструктуры у отдельных производителей и организаций могут отличаться, поэтому ИСО/ТС 22600 определяет эти процессы и модели на информационном и вычислительном уровне представления. Его спецификации являются открытыми, платформенно-независимыми, переносимыми и масштабируемыми, что позволяет применять его в разных условиях оказания медицинской помощи и в разных странах, где национальные и профессиональные нормы могут отличаться.

Согласно настоящему стандарту для управления принятием решений о доступе по запросу на получение данных ЭМК применяется логический подход, предложенный в ИСО/ТС 22600. Однако определение актуальных моделей политик, атрибутов или значений атрибутов, которые нужны для представления конкретных экземпляров политик, или способа технической реализации логического подхода, предложенного в ИСО/ТС 22600, в какой-либо организации или в регионе выходит за рамки настоящего стандарта.

В дополнение к настоящему стандарту ИСО/ТС 21298 определяет совокупности структурных и функциональных ролей, которые могут использоваться в качестве международных для согласования политик и отображения одной политики на другую (то есть на этапе согласования решения о представлении доступа). В настоящем стандарте учитывается, что эти и другие стандартные словари будут постоянно улучшать интероперабельность политик доступа. Однако он не может потребовать использования конкретного контролируемого словаря, поскольку пока что ни один из них не является формальным стандартом.

3.4 Требования безопасности, специфичные для передачи ЭМК

ИСО/ТС 18308 содержит большое число медико-правовых и этических требований, специфичных для ЭМК. Соответствие этим требованиям в основном достигается с помощью специальных классов и атрибутов эталонной информационной модели (опубликована в ИСО 13606-1). В таблице 1 указаны требования, которые в наибольшей мере учитываются в настоящем стандарте.

Таблица 1 — Перечень требований, опубликованных в ИСО/ТС 18308 и относящихся к безопасности передачи ЭМК

COC1.2	Архитектура ЭМК (АЭМК) должна обеспечивать права потребителя на доступ к данным ЭМК с учетом требований законодательства
COC1.3	АЭМК должна позволять потребителю включать в ЭМК информацию о самолечении, оценку своего состояния здоровья, степень удовлетворения, ожидания и комментарии
COM2.4	АЭМК должна обеспечивать отслеживание процессов обмена, включая аутентификацию, в целях идентификации мест передачи и приема выписок из ЭМК. Такое отслеживание необходимо для учета процессов объединения данных
PRS1.2	АЭМК должна обеспечивать категорирование всей ЭМК или ее разделов как доступных только авторизованным пользователям и/или для определенных целей, включая ограничения на уровне чтения, записи, изменения, верификации и передачи/раскрытия данных и записей
PRS1.3	АЭМК должна поддерживать ограничения конфиденциальности и неприкосновенности личной информации как на уровне наборов данных, так и на уровне отдельных атрибутов
PRS2.2	АЭМК должна обеспечивать возможность получения, регистрации и отслеживания статуса информированного согласия[1)] на доступ к ЭМК или ее разделам с определенными целями
PRS2.4	АЭМК должна обеспечивать возможность регистрации срока действия каждого информированного согласия

Окончание таблицы 1

PRS3.1	АЭМК должна обеспечивать возможность определения, присвоения, изменения и отмены прав доступа ко всей ЭМК или к ее разделам
PRS3.3	АЭМК должна обеспечивать возможность разрешения и ограничения доступа ко всей ЭМК или к ее разделам в соответствии с имеющимся информированным согласием и с действующими правилами доступа
PRS3.4	АЭМК должна обеспечивать возможность раздельного управления разрешениями на добавление или изменение ЭМК и разрешениями на доступ к ЭМК
PRS5.1	АЭМК должна обеспечивать возможность регистрации доступа и изменения информации в ЭМК или в ее разделах
PRS5.2	АЭМК должна обеспечивать возможность регистрации характера каждого акта доступа и/или изменения
STR2.10	АЭМК должна обеспечивать расширенные возможности хранения и извлечения информации о лечении пациента. Она должна, как минимум, позволять регистрацию всех структурированных и неструктурированных данных, касающихся: - прочих событий, - раскрытия информации и представления информированного согласия.

[1)] В настоящее время признается, что необходимо учитывать также неявное или подразумеваемое согласие.

4 Общая модель политик доступа к ЭМК

4.1 Факторы, требующие учета при специфицировании политик доступа к ЭМК

При включении требований, указанных в 3.4, в настоящий стандарт учитывалось, что в большинстве действующих клинических информационных систем и систем ведения ЭМК реализуются относительно простые меры по контролю доступа, обычно адекватные нуждам отдельной организации. Лишь немногие из них интероперабельны с программным обеспечением других поставщиков или с такими смежными системами, как поддержка принятия решений, потоки работ или системы выдачи отчетов. В системах нового поколения возможности конфигурирования политик доступа постоянно расширяются, но для обеспечения распределенной обработки ЭМК необходимо иметь интероперабельные спецификации политик и их интероперабельную реализацию. Представляется, что большинство поставщиков, служб и сетей здравоохранения придерживаются пошагового подхода к тому, чтобы сделать реализуемые ими политики контроля доступа более развитыми.

В любой региональной сети здравоохранения имеется значительное число высокоуровневых политик управления доступом к ЭМК. В настоящее время они существуют в основном на бумаге или в форме ненастраиваемого программного кода приложений и серверов, но в будущем они будут представлены в форме интероперабельных политик доступа в соответствии с архитектурой, предложенной в ИСО/ТС 22600. Ниже перечислены некоторые образцы, которые могут быть указаны в таких политиках и учитываться при принятии решения о доступе к ЭМК.

Политики организации, национальные и профессиональные политики могут формулироваться с использованием следующих атрибутов:

Атрибуты пользователя:

- фамилия, имя, отчество и идентификатор;
- профессия, специальность, квалификация;
- функциональная роль;
- отделение или клиническая специальность в этом отделении;
- организация, в которой он состоит.

Атрибуты доступа:

- дата и время;
- место;
- физическое устройство;
- сеть или иная среда информационного взаимодействия;

- используемые механизмы и степень применения шифрования;
- используемый метод аутентификации.

Политики организации могут также утверждать разрешения доступа:

- к информации о конкретном пациенте;
- к архетипу;
- к запрошенной операции (чтение, запись, изменение, передача данных, запрос и т. д.).

Политики, специфичные для ЭМК, могут предоставлять разрешение или отказывать в нем:

a) поименованным/идентифицированным сторонам:

- для доступа к ЭМК в целом;
- для назначения конкретной функциональной или структурной роли (например, для указания персонального уполномоченного представителя в организации здравоохранения);

b) в зависимости от специфичных условий оказания медицинской помощи (например, отделение, специальность);

c) специфичным функциональным ролям;

- для доступа к конкретным архетипам;
- для доступа к конкретным компонентам ЭМК;
- для доступа к данным определенной категории;
- для выполнения специфичных функций обработки ЭМК (например, чтение, запись, изменение, передача информации, запрос);

d) специфичным целям доступа:

- например, непосредственное оказание медицинской помощи, обеспечение оказания медицинской помощи, преподавание, исследовательская работа;
- требующим выполнения определенных условий (например, должно быть обеспечено формальное подписанное информированное согласие).

Спецификация всего спектра политик доступа, которые должны иметься в организации, выходит за рамки настоящего стандарта. Он определяет общую спецификацию представления и передачи тех частей политики доступа, которые непосредственно связаны с содержанием любой заданной ЭМК (целевые политики). Нередко они отражают волю пациента в части раскрытия персональной информации.

Передача специфичного информированного согласия и политик доступа, выражающих волю пациента или его представителей, является важным аспектом передачи ЭМК и интероперабельности. Такие политики вносят свой вклад в общую процедуру принятия решения об удовлетворении запроса на доступ к ЭМК и должны передаваться получателю результата запроса вместе с данными, извлеченными из ЭМК, чтобы получатель мог применить эти политики для управления любым последующим доступом к этим данным в своей организации.

Общая модель представления политик информированного согласия и доступа, выражающих волю пациента или других сторон, определена в разделе 6 настоящего стандарта. Политики, специфичные для ЭМК и которые должны быть включены в выписку EHR_EXTRACT, могут быть представлены с помощью модели, описанной в разделе 6. Эта модель свободно расширяется, что позволяет обрабатывать дополнительные спецификации политик, не предусмотренные настоящим стандартом. Поскольку ИСО/ТС 22600-3 определяет интероперабельную модель политики доступа, которая может использоваться для этой цели, то в разделе 6 описана также модель на языке UML, чтобы информационные системы, удовлетворяющие настоящему стандарту, заодно удовлетворяли и ИСО/ТС 22600.

В эталонной информационной модели, описанной в стандарте ИСО 13606-1, каждый компонент данных (RECORD_COMPONENT), содержащийся в выписке EHR_EXTRACT, включает в себя необязательный атрибут идентификатора политики (Policy_ID), который можно использовать для ссылки на такие политики с любой степенью детализации в иерархии структуры ЭМК. Поэтому каждый компонент RECORD_COMPONENT может ссылаться на любое число политик доступа или деклараций информированного согласия, определяющих привилегии и профили принципалов (пользователей, агентов, компонентов программного обеспечения, устройств, делегированных действующих лиц и т. д.), которые впоследствии потребуются для доступа к этому элементу.

Необходимо принять во внимание, что некоторые политики могут применяться к конкретному элементу RECORD_COMPONENT, входящему в ЭМК, а другие — к ЭМК в целом.

4.2 Политики доступа к ЭМК: минимальная спецификация для интероперабельности

4.2.1 Общие положения

Информационная модель, описанная в разделе 6 и предназначенная для представления и передачи информации о политике доступа, намеренно оставлена очень общей, чтобы она могла охватить все разнообразие критериев политик, уже предложенных в разных странах и в региональных сетях организаций здравоохранения. Стандартизованные словари для многих из возможных атрибутов в настоящее время еще не определены. Поэтому модель политик, описанная в разделе 6, способна лишь частично повлиять на интероперабельность политик.

Значительное число существующих и унаследованных систем может оказаться не в состоянии интерпретировать более детальные спецификации политик, а многие региональные системы здравоохранения не смогут определить такие политики в течение ближайших лет. Поэтому в качестве дополнения к общей модели политик, описанной в разделе 6, настоящий стандарт определяет два словаря данных, которые могут помочь в принятии решений в политике доступа и обеспечить базовый уровень интероперабельности политик доступа, хотя и с невысоким уровнем детализации.

Этими двумя словарями являются:

- классификация категорий данных ЭМК (компонентов RECORD_COMPONENT);
- высокоуровневая классификация лиц, запрашивающих ЭМК, и получателей ЭМК, составленная в форме набора функциональных ролей.

4.2.2 Определение «необходимости знания» при обработке данных ЭМК

В условиях конкретной клиники (например, в коллективе медицинских работников, оказывающих непосредственную помощь пациенту, и между такими коллективами) нормой является открытый совместный доступ персонала к информации медицинской карты. Большинство пациентов обычно согласны с этим, но многие из них удивляются тому, насколько мала та часть их медицинских карт, которая востребована сотрудниками клиники, в то время как такой совместный доступ мог бы повысить безопасность и преемственность медицинской помощи.

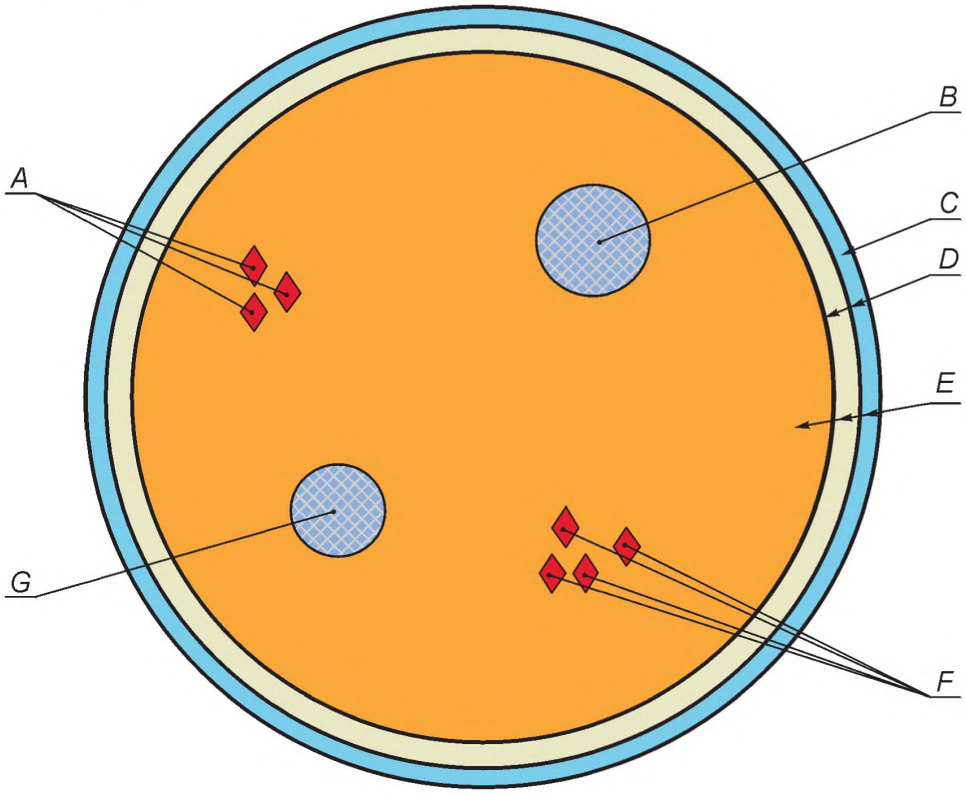
Комплексный внутренний контроль доступа, дифференцирующий доступ персонала к данным, хранящимся в медицинских картах (бумажных или электронных), практикуется в очень немногих современных информационных системах здравоохранения. Даже в том случае, если бы определение многочисленных детальных политик доступа считалось полезным, на практике потребовался бы весьма длительный срок, чтобы системы здравоохранения, национальные службы здравоохранения и миллионы пациентов договорились бы об адекватных политиках контроля доступа к данным ЭМК, а затем были бы реализованы программные компоненты, которые могли бы выполнять многие сложные преобразования политик в реальном времени. Управление этими политиками по мере эволюции требований клинической помощи каждому пациенту также показалось бы очень сложным.

Теоретически можно определить (усилиями пациентов или других лиц) набор политик доступа, обеспечивающих многоуровневый доступ к каждой конкретной ЭМК, но на практике большинство клиник применяет подход, при котором по умолчанию права доступа к медицинской карте предоставляются каждому медицинскому работнику, который имеет законный интерес к данному пациенту. (Определение понятия законного интереса может зависеть от конкретной организации и не рассматривается в настоящем стандарте.) Однако при этом вполне допускается, что пациентам и медицинским работникам может время от времени требоваться ограничение доступа к некоторым более личным и чувствительным данным электронной медицинской карты. В большинстве служб здравоохранения общей практикой является выделение некоторых разделов ЭМК, к которым могут иметь доступ только специализированные клиники (например, кожно-венерологические диспансеры).

Способ наделения определенных клиник специфичными правами доступа или присваивания особых категорий чувствительности определенным разделам ЭМК значительно отличается от способа деления ЭМК на разделы, способствующие навигации по ее содержанию или относящиеся к определенной клинической специальности, например, выделение в ЭМК разделов, связанных с онкологическим заболеванием или диабетом.

В ИСО 27799 рассмотрены проблемы определения чувствительных элементов персональной медицинской информации. Субъекты медицинской информации, а также клиники, располагающие этими данными или нуждающиеся в них, нередко судят о таком определении, исходя из субъективных представлений, которые со временем могут меняться. Поэтому в ИСО 27799 представлены классификация и категорирование таких активов, как персональная информация, с позиций того, кому такую информацию необходимо знать.

На рисунке 3 показан пример логического деления ЭМК на части с позиции «необходимости знания», при которой классификация уровней конфиденциальности (категорирование) представлена по отношению к классам пользователей и конкретных клинических условий.



A — личные данные, доступные участковому терапевту
B — данные, доступ к которым разрешен только персоналу кожно-венерологического диспансера
C — данные, доступные административному персоналу
D — данные, доступные вспомогательному медицинскому персоналу
E — данные, доступные медицинскому персоналу, оказывающему непосредственную медицинскую помощь
F — личные данные, доступные только нескольким названным сторонам
G — данные, доступные только персоналу тюремной больницы

Рисунок 3 — Иллюстрация доменов доступа на примере ЭМК

На рисунке 3 предполагается, что пациент имеет полный доступ к своей ЭМК. Большая часть ЭМК данного пациента доступна любой стороне, оказывающей пациенту непосредственную медицинскую помощь. Однако эта ЭМК содержит несколько закрытых элементов; некоторые из них доступны врачу общей практики (семейному врачу), наблюдающему данного пациента, а другие — отдельному списку поименованных сторон. ЭМК содержит также некоторые элементы, созданные кожно-венерологическим диспансером и доступные только ему, а также элементы, доступ к которым разрешен тюремной службе медицинской помощи, — и те и другие могут быть доступны только сторонам, наделенным адекватными дополнительными привилегиями доступа к этим элементам. (Однако пациент может по своему желанию предоставить другим сторонам право доступа к этим элементам ЭМК.) Одним из аспектов привилегий доступа является назначение медицинской организацией определенных ролей медицинскому специалисту, которые позволят в экстренной ситуации расширить его привилегии по сравнению с теми, которыми он наделен в обычной ситуации. Подобное расширение прав в экстренной ситуации может, например, обеспечить медицинскому специалисту доступ к большему числу ЭМК, чем при обычной работе. (Такое расширение прав в экстренной ситуации должно специально регистрироваться и регулярно разбираться.)

Некоторые части ЭМК могут быть свободно доступны вспомогательным работникам, которым могут понадобиться результаты определенных клинических исследований, чтобы выполнять такую деятельность, как планирование или новые исследования.

Очень малая часть ЭМК может стать доступной административному персоналу. Медрегистраторы, секретари и диспетчеры должны обладать знанием только некоторой ключевой информации о пациенте, чтобы выполнять свою роль в оказании эффективной медицинской помощи, например, знать, что пациенту требуется специальное санитарное просвещение или что ему необходим кислород 24 %, или каталка для транспортировки в отделение лучевой диагностики.

В этом примере не показано, как запретить самому пациенту доступ к некоторым элементам его ЭМК, но такие возможности, если они предусмотрены действующим законодательством, могут быть реализованы в рамках модели политик, описанной в разделе 6. Например, пациенту могут стать недоступными сведения ЭМК, конфиденциально сообщенные его близкими.

При определении детального набора политик для определенной категории пациентов, специальных клинических условий или в связи с тем, что какой-то пациент более других озабочен безопасностью своей ЭМК, реализация распределенной системы ведения ЭМК должна осуществляться таким образом, чтобы в обозримом будущем большинство случаев удовлетворялось с помощью ограниченного набора параметров по умолчанию и достаточно простой схемы применения политик. Это связано с тем, что детальный набор политик может не допускать непосредственную интерпретацию и встраивание в систему ведения ЭМК получателя электронной медицинской карты, даже если информация об этих политиках может быть передана стандартизованным образом.

В дополнение к общему представлению информации политики доступа к ЭМК (приложение А) настоящий стандарт описывает также спецификацию минимальной базы для передачи информации о чувствительности данных ЭМК в составе выписки EHR_EXTRACT с помощью указания категории безопасности каждого ее компонента RECORD_COMPONENT, взятой из классификации, описанной в 5.1. Эта классификация соответствует различным подчиненным доменам данных ЭМК, показанным на рисунке 3.

На практике любая конкретная система ведения ЭМК может иметь другие механизмы категорирования данных электронной медицинской карты или назначения им других уровней безопасности. Настоящий стандарт не требует, чтобы системы ведения ЭМК обязательно использовали классификацию категорий безопасности, определенную в 5.1. Достаточно, если при создании объекта EHR_EXTRACT будет обеспечена возможность отображения своих категорий безопасности на эту классификацию.

4.2.3 Функциональные роли для доступа к данным ЭМК

Для обеспечения принятия решения о доступе требуется, чтобы профиль объявленного получателя ЭМК и цель его доступа к ЭМК соответствовали политикам, применяемым к данной ЭМК поставщиком ЭМК, включая категории специфичных запрошенных компонентов RECORD_COMPONENT.

В связи с этим профиль запрашивающего лица и/или получателя ЭМК должен быть указан интероперабельным способом. Как уже отмечалось ранее, требования, регламентирующее законодательство, атрибуты и словари данных, используемые для этой цели в каждой стране, могут быть разными и пока что не могут быть стандартизованы.

Для обеспечения базового уровня интероперабельности и минимального соответствия настоящему стандарту требуется, чтобы любой запрос на получение объекта EHR_EXTRACT содержал в качестве параметра функциональную роль предполагаемого получателя ЭМК из числа указанных в 5.2.

Это множество функциональных ролей идентично тому, что указано в ИСО/ТС 21298. В настоящий стандарт оно включено в качестве нормативной спецификации.

Зависимость между функциональной ролью и категорией данных ЭМК, которая влияет на принятие решения о представлении доступа или отказе в нем либо на фильтрацию содержания выписки EHR_EXTRACT, определена в 5.3.

Это отображение обеспечивает базовый способ (с начальным уровнем детализации) ограничения рамок доступа к ЭМК в зависимости от типа стороны, запрашивающей доступ. В случае, когда интероперабельная спецификация профиля запрашивающего лица определяется на местном или национальном уровне, всегда можно добавить дополнительные детали. Пример сочетания базового отображения с небольшим числом дополнительных спецификаций в целях получения более детального набора ограничений доступа приведен в разделе 6.

5 Интероперабельность журнала аудита

Регистрация деталей взаимодействия с системой ведения ЭМК для аудита является общепризнанным требованием. Однако способ реализации такой регистрации в журнале аудита достаточно специфичен для каждой системы ведения ЭМК, что частично обусловлено используемым способом хранения данных (например, базой данных) и, возможно, особенностями регионального или национального законодательства. Формальные стандарты интероперабельности журнала аудита и передачи его содержания пока что отсутствуют.

Требования к интероперабельности журнала аудита должны быть описаны в ИСО 27789, находящемся в стадии разработки. Этот стандарт определит события, инициирующие запись в журнал аудита, и элементы данных для записей в журнале доступа к ЭМК. (Спецификация содержания журналов аудита была опубликована в 2004 году как неформальный проект документа IETF RFC 3881.)

Однако становится все более очевидным, что предоставление пациентам возможности узнать, кто именно получал доступ к их ЭМК, является не только формальным правом, но и может дисциплинировать медицинских работников, которые пользуются доступом к ЭМК, данные которых не входят в их профессиональные обязанности.

Хотя отдельные системы ведения ЭМК могут обеспечить некоторую степень доступа к журналу аудита, в настоящее время такой доступ обычно предоставляется администраторам баз данных с помощью инструментов и интерфейсов, совершенно неподходящих для того, чтобы пациенты просматривали историю доступа к своим ЭМК. В сценарии распределенного доступа к ЭМК (с разделением информации) журналы доступа к ЭМК неизбежно также будут распределенными.

Поэтому необходимы интероперабельные спецификации базового набора данных, который может быть предоставлен по запросу пациента или его представителя на получение списка событий доступа к его ЭМК. Соответствующие определения даны как в информационной модели просмотра журнала аудита (раздел 7), так и в модели интерфейса запроса и ответа (ИСО 13606-5).

Поскольку известно, что немногие действующие системы удовлетворяют требованию интероперабельности журнала аудита, то соответствие этому требованию рассматривается отдельно от соответствия требованиям остальной части настоящего стандарта. Должно ли это дополнительное требование выполняться или нет, остается на усмотрение региональных или национальных политик.

Представление журнала аудита для пациента отнюдь не является средством изучения журнала в процессе формального расследования доступа к системе ЭМК. Настоящий стандарт не содержит каких-либо интероперабельных спецификаций, предназначенных для таких расследований.

6 Связь со стандартом ENV 13606-3

Правила распространения, включенные в стандарт ENV 13606, опубликованный в 2000 году, предусматривали создание детальной аналитической базы для разработки требований, которые должны удовлетворяться при санкционировании передачи данных ЭМК. Анализ опыта ее применения, проведенный группой разработчиков этого стандарта (EHRcom), привел к выводу, что эту детальную базу трудно реализовать на практике по нескольким причинам:

- некоторые аспекты ее спецификации, например «WHY» (цель требования передачи ЭМК), определены с помощью текстовых атрибутов без формализованного словаря данных, что препятствует достижению интероперабельности;
- общая базовая структура предусматривала гораздо больше деталей контроля доступа, чем реализовано в большинстве современных систем ведения ЭМК, и ее реализация была бы одновременно и дорогой, и трудной;
- она потребовала бы от медицинских работников значительных дополнительных усилий по заполнению экземпляров правил в процессе оперативного ввода данных в ЭМК;
- во многих компьютеризованных системах здравоохранения принимались и принимаются общие меры безопасности, и добавление к ним средств, специфичных для ЭМК, рассматривалось бы как необоснованное.

С 2000 года многие службы здравоохранения разработали стратегии по обеспечению безопасности самих информационных систем здравоохранения и обменов данными между этими системами.

Многие программные продукты в настоящее время включают в себя такие общие компоненты безопасности, как службы сертификатов и инфраструктура открытых ключей, либо имеют интерфейсы к таким компонентам. Стандарты информационной безопасности, опубликованные после 2000 года, затрагивают многие из аспектов, которые тогда было необходимо определить в правилах распространения.

В настоящем стандарте предлагается использовать или эти стандарты, общие для многих отраслей, или общие меры информационной безопасности, специфичные для здравоохранения в целом, и описать только те возможности, которые специфичны для передачи ЭМК — прежде всего разрешения доступа, которые ассоциируются с каждой ЭМК. Наиболее общим примером такого подхода будет служить учет воли пациента (субъекта данных) по раскрытию информации.

Более детальное описание отличий от стандарта ENV 13606 приведено в приложении В.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Информатизация здоровья

ПЕРЕДАЧА ЭЛЕКТРОННЫХ МЕДИЦИНСКИХ КАРТ

Часть 4

Безопасность

Health informatics. Electronic health record communication. Part 4. Security

Дата введения —2012—08—01

1 Область применения

Настоящий стандарт описывает методологию специфицирования привилегий, необходимых для доступа к данным ЭМК. Эта методология является частью общей архитектуры передачи ЭМК, описанной в ИСО 13606-1.

В настоящем стандарте рассматриваются требования, которые специфичны для передачи ЭМК и для представления и передачи сопутствующей информации, которая необходима для принятия решения о доступе. В нем также содержатся ссылки на общие требования информационной безопасности, применимые к передаче ЭМК, и указания на технические решения и стандарты, описывающие детали служб, удовлетворяющих этим требованиям.

Примечание — Требования безопасности, предъявляемые к системам ведения ЭМК, но не имеющие отношения к передаче ЭМК, не рассматриваются в настоящем стандарте.

2 Соответствие

Соответствие настоящему стандарту требуется в одном из двух случаев:

- использование в качестве основы для принятия решения о доступе минимума крупных категорий чувствительности данных ЭМК и функциональной роли получателя;
- использование общей модели политик для передачи детальной информации политики доступа, отражающей волю субъекта медицинской помощи и/или региональные или национальные методические указания, которые должны совместно применяться в процессе распространения ЭМК.

Настоящей стандарт включает в себя также необязательное соответствие спецификации интероперабельного представления журнала аудита.

Для «минимального соответствия» необходимо использовать классификацию компонентов RECORD_COMPONENT выписки EHR_EXTRACT, определенную в 5.1. Любой запрос на доступ к выписке EHR_EXTRACT должен в качестве параметра включать в себя функциональную роль предполагаемого получателя ЭМК, определенную в 5.2. Соотношение между функциональной ролью и категорией информации ЭМК, используемое для принятия решения о разрешении доступа или отказа в доступе, должно удовлетворять отображению, определенному в 5.3.

Для «нормального соответствия» необходимо, чтобы выписка EHR_EXTRACT включала в себя по значению или по ссылке общее представление информации каждой политики, распространяющейся на передаваемые данные ЭМК, либо явно соответствующее 6.3, либо логически соответствующее 6.4 в сочетании с другими опубликованными стандартами представления политик доступа. В случае если поставщик ЭМК уверен, что получатель ЭМК уже имеет непосредственный доступ к информации данной политики, то эта политика может использоваться по ссылке и не включаться в выписку EHR_EXTRACT.

Издание официальное

Нормальное соответствие может дополнительно требовать обязательство выполнения требований минимального соответствия.

Если в дополнение к нормальному соответствию требуется интероперабельное представление журнала аудита, то для подобного «расширенного соответствия» должна использоваться информационная модель такого представления, описанная в 7.

3 Термины и определения

В настоящем стандарте применены следующие термины с соответствующими определениями:

3.1 **контроль доступа** (access control): Средства, с помощью которых ресурсы системы обработки данных предоставляются только авторизованному субъекту по авторизованным каналам.

Примечание — Адаптировано из ИСО/МЭК 2382-8:1998.

3.2 **политика доступа** (access policy): Процесс, устанавливающий обязательства авторизованного контроля доступа к ресурсу.

3.3

отчетность (accountability): Свойство, означающее, что все действия каждого субъекта безопасности с каждым объектом безопасности могут быть изучены в целях установления реальной ответственности за действия с этим объектом.

[ENV 13608-1:2000]

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

3.5 **авторизация** (authorization): Процесс предоставления прав.

3.6 **уполномоченное лицо** (authority): Субъект, ответственный за выпуск сертификатов.

3.7

доступность (availability): Свойство доступности и возможности беспрепятственного использования авторизованным субъектом.

[ИСО 7498-2:1989, определение 3.3.11]

3.8 **конфиденциальность** (confidentiality): Процесс, гарантирующий, что информация доступна только авторизованным субъектам.

3.9 **выписка из ЭМК** (EHR extract): Часть электронной медицинской карты или вся карта, передаваемая в соответствии с требованиями настоящего стандарта.

3.10 **поставщик ЭМК** (EHR provider): Субъект, законно обладающий данными электронной медицинской карты и способный передать их другому соответствующему субъекту.

3.11 **получатель ЭМК** (EHR recipient): Субъект, получающий данные электронной медицинской карты от поставщика ЭМК.

3.12 **лицо, запрашивающее ЭМК** (EHR requester): Субъект, инициирующий запрос поставщику ЭМК на передачу данных электронной медицинской карты получателю ЭМК.

3.13

идентификация (identification), **аутентификация идентичности** (identity authentication), **проверка идентичности** (identity validation): Выполнение проверок, позволяющих системе обработки данных опознать субъект.

[ИСО/МЭК 2382-8:1998, определение 08.04.12]

3.14

идентификатор (identifier): Информационный объект, используемый для объявления идентичности перед тем, как получить подтверждение соответствия от определенного аутентификатора.

[ENV 13608-1:2000]

3.15

ключ (key): Последовательность символов, управляющая операциями шифрования и дешифровки.
[ИСО 7498-2, определение 3.3.32]

3.16

политика (policy): Комплекс юридических, методических, организационных, функциональных и технических обязательств по обмену информацией и совместной деятельности.
[ИСО/ТС 22600-1:2006, определение 2.13]

3.17 **привилегия** (privilege): Право, предоставленное субъекту уполномоченным лицом.

3.18

инфраструктура открытых ключей (public key infrastructure), **ИОК** (PKI): Инфраструктура, используемая держателем ключа в отношениях с доверяющей стороной, которая позволяет доверяющей стороне использовать сертификат, относящийся к держателю ключа, по крайней мере для одного применения, используя сервис системы обеспечения безопасности на основе открытого ключа. ИОК включает в себя уполномоченное лицо по сертификатам, структуру данных сертификатов, средства получения доверяющей стороной текущей информации о статусе отзыва сертификата, политике сертификатов и способах проверки соответствия практике сертификации.
[ИСО 17090-1:2008, определение 3.3.18]

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

3.20 **чувствительность** (sensitivity): Мера ценности, присвоенная информации для обозначения необходимой степени защиты.

3.21

безопасность (security): Сочетание доступности, конфиденциальности, целостности и отчетности.
[ENV 13608-1:2000]

3.22

политика безопасности (security policy): Утвержденный план или способ действий по обеспечению информационной безопасности.
[ИСО/МЭК 2382-8:1998, определение 08.01.06]

3.23

сервис безопасности (security service): Сервис, предоставляемый уровнем взаимодействия открытых систем, обеспечивающий надлежащую степень безопасности системы или передачи данных.
[ИСО 7498-2:1989, определение 3.3.51]

3.24 **субъект медицинской помощи** (subject of care): Лицо, обращающееся за получением, получающее или получившее медицинскую помощь.

Примечание — Адаптировано из стандарта ЕН 14822-2:2005.

3.25 **цель** (target): Ресурс, к которому запрашивается доступ.

4 Обозначения и сокращения

ADL — язык определения архетипов (archetype definition language);
ЭМК — электронная медицинская карта (electronic health record, EHR);
АЭМК — архитектура электронных медицинских карт (electronic health record architecture, EHRA);

ИОК — инфраструктура открытых ключей (public key infrastructure, PKI);

УПКД — управление привилегиями и контроль доступа (privilege management and access control, PMAC);

UML — унифицированный язык моделирования (unified modelling language).

5 Чувствительность компонентов ЭМК и функциональные роли

5.1 Чувствительность элемента RECORD_COMPONENT

Согласно определению ИСО 13606-1, если категория чувствительности компонента RECORD_COMPONENT, входящего в состав выписки EHR_EXTRACT, указана, то она должна принимать одно из значений CS_SENSITIVITY, указанных в таблице 2.

Таблица 2 — Значения CS_SENSITIVITY, используемые для атрибута категории чувствительности компонента RECORD_COMPONENT

Значение CS_SENSITIVITY	Категория чувствительности	Описание предполагаемого доступа к компоненту RECORD_COMPONENT данной категории чувствительности
Личные сведения (personal)	5	Сугубо личные сведения субъекта медицинской помощи, которые могут предоставляться только отдельным наиболее доверенным лицам, или иные сведения, доступные только самому субъекту (и другим лицам при авторизации однократного доступа)
Специальная медицинская помощь (privileged care)	4	Доступ разрешен только небольшой группе людей, лично предоставляющих пациенту медицинскую помощь, например, бригаде медицинских работников или руководителям отделения (необходимо указать особые клинические условия, например, психиатрическая клиника)
Медицинская помощь (clinical care)	3	Эта категория присваивается по умолчанию обычному доступу в лечебно-профилактическом учреждении (например, большая часть медицинского персонала, непосредственно оказывающего медицинскую помощь пациенту, должна иметь возможность доступа почти ко всей ЭМК)
Планирование медицинской помощи (clinical management)	2	Менее чувствительные компоненты RECORD_COMPONENT, доступ к которым может требоваться большому числу сотрудников, не все из которых принимают активное участие в лечении пациента (например, персоналу отделения лучевой диагностики)
Управление ресурсами медицинской помощи (care management)	1	Компоненты RECORD_COMPONENT, доступ к которым может требоваться значительному числу административных работников в целях управления представлением ресурсов медицинской помощи конкретному пациенту

5.2 Функциональные роли

Функциональная роль каждого предполагаемого получателя ЭМК должна принимать одно из значений, указанных в таблице 3. Эти значения приведены в соответствие с функциональными ролями, определенными в ИСО/ТС 21298.

Таблица 3 — Список функциональных ролей

Функциональная роль	Краткое описание
Субъект медицинской помощи (subject of care)	Основной субъект данных электронной медицинской карты
Представитель субъекта медицинской помощи (subject of care agent)	Например, родитель, попечитель, лицо, обеспечивающее уход, или иной законный представитель
Личный врач (personal healthcare professional)	Медицинский специалист или специалисты, наиболее близкие пациенту, нередко участковый терапевт

Окончание таблицы 3

Функциональная роль	Краткое описание
Доверенный медицинский работник (privileged healthcare professional)	Медицинский специалист, названный субъектом медицинской помощи или назначенный руководством лечебно-профилактического учреждения (когда такое назначение регулируется законом, принятой практикой и т. д., например, при оказании экстренной медицинской помощи)
Лечащий медицинский работник (healthcare professional)	Лицо, непосредственно оказывающее медицинскую помощь пациенту
Вспомогательный работник (health-related professional)	Лицо, косвенно вовлеченное в оказание медицинской помощи, санитарное просвещение, научную работу
Администратор (administrator)	Любое другое лицо, обеспечивающее предоставление медицинской помощи пациенту

5.3 Отображение функциональной роли на категорию чувствительности элемента RECORD_COMPONENT

При принятии решения о доступе должна использоваться таблица 4, указывающая при какой функциональной роли, указанной в запросе электронной медицинской карты, получатель ЭМК может получить доступ к элементу RECORD_COMPONENT, имеющему определенную категорию чувствительности.

Таблица 4 — Отображение функциональных ролей на категорию чувствительности элемента RECORD_COMPONENT

Функциональная роль	Категория чувствительности элемента RECORD_COMPONENT				
	Управление ресурсами медицинской помощи	Планирование медицинской помощи	Медицинская помощь	Специальная медицинская помощь	Личные сведения
Субъект медицинской помощи	Д	Д	Д	Д	Д
Представитель субъекта медицинской помощи	Д	Д	Д	Д	Д
Личный врач	Д	Д	Д	Д	Д
Доверенный медицинский работник	Д	Д	Д	Д+	++
Лечащий медицинский работник	Д	Д	Д	—	—
Вспомогательный работник	Д	Д	—	—	—
Администратор	Д	—	—	—	—

Д — в отсутствие других ограничений политики, описанных в разделе 7, будет разрешен доступ к компоненту RECORD_COMPONENT данной категории чувствительности;

\+ — доступ будет разрешен, если получатель ЭМК имеет ту же специальность или принадлежит к той же клинической службе, которой был создан компонент RECORD_COMPONENT, например, является сотрудником кожно-венерологического диспансера или тюремной больницы, что должно быть указано в атрибуте условий оказания помощи (service_setting) объекта композиции COMPOSITION, определенного в эталонной информационной модели, описанной в ИСО 13606-1. Доступ может быть также разрешен в ситуациях, требующих скорую или неотложную помощь, если такая возможность авторизована;

++ — в определенных условиях оказания медицинской помощи, например, в Вооруженных силах некоторых стран, доступ к сугубо личной информации может иногда разрешаться с ведома доверенных медицинских работников.

6 Представление информации о политике доступа в выписке EHR_EXTRACT

6.1 Общие положения

Информация о политике доступа, которая должна быть передана получателю ЭМК, содержится в выписке EHR_EXTRACT в виде одного или нескольких объектов композиций COMPOSITION, вложенных в объект тома FOLDER, специально выделенный для политик доступа. Настоящая спецификация не предназначена для описания способа, которым программные компоненты могут представить этот вид информации в системе ведения ЭМК или в компонентах безопасности, обслуживающих эту систему. Она призвана описать общий способ включения этой информации в выписку EHR_EXTRACT, с тем чтобы получатель ЭМК мог обеспечить выполнение той же самой воли, выраженной в информированном согласии при доступе к ЭМК, или передать ее другим участникам доступа.

Примечание — Композиции COMPOSITION могут быть аттестованы, и свидетельство аттестации может быть включено в выписку EHR_EXTRACT.

Том FOLDER не обязателен, поскольку не всегда требуется передавать информацию о политике от одной стороны к другой, например, в случае, когда стороны уже имеют общий доступ к такой информации или для данной ЭМК не заданы уникальные политики.

Каждая политика представляется в виде отдельной композиции COMPOSITION, архетип которой должен соответствовать спецификации 6.3. Каждый экземпляр имеет вид выдержки из политики и должен создаваться для передачи дискретной спецификации разрешения или отказа в доступе ко всей электронной медицинской карте или к ее части, которая считается подходящей для включения в выписку EHR_EXTRACT в целях последующего применения получателем ЭМК.

Чтобы упростить обеспечение соответствия стандартам серии ИСО 13606, в настоящем стандарте вместо отдельной информационной модели политик используется представление информации о политике в виде композиций COMPOSITION, удовлетворяющих требованиям ИСО 13606-1. Информация об авторстве, создании, истории версий и аттестации информации о политике доступа представляется тем же способом, что и в других компонентах RECORD_COMPONENT выписки EHR_EXTRACT. Поэтому возможно, например, включить по значению или по ссылке подпись пациента, относящуюся к политике доступа, или указать, что политика доступа заменяет ранее переданную. Выписка EHR_EXTRACT может использоваться для передачи только информации о политике, без включения в нее каких-либо других данных ЭМК. В ситуации, когда взаимодействующие стороны имеют общую архитектуру информированного согласия и авторизации, вместо логического представления информационной модели политики в соответствии с 6.4 может использоваться и передаваться представление, описанное в ИСО/ТО 22221 (УПКД).

Архетип композиции COMPOSITION, содержащей политики доступа, состоит из трех объектов разделов SECTION и одного дополнительного объекта подраздела ENTRY, представляющего срок действия политики. Этот срок задается как интервал времени, начало или конец которого могут быть пустыми, что означает соответственно немедленный ввод в действие или неопределенную продолжительность.

Раздел спецификации запроса SECTION используется для определения типа сценария запроса, к которому применяется данная политика. Тип запроса может быть задан в терминах конкретных функциональных ролей (см. раздел 5), функциональных обязанностей (подобных функциональным ролям, определенным для местного применения), структурных ролей, условий оказания медицинской помощи или медицинских специальностей. Отдельные стороны (например, лица, организации, устройства, представители) могут быть идентифицированы с помощью идентификаторов экземпляра, которые могут быть отображены на более полное описание стороны в объекте DEMOGRAPHIC_EXTRACT (см. ИСО 13606-1). Любые другие характеристики, которые должны быть определены в запросе, могут быть указаны как список строк. Каждый из этих способов определения сценария запроса представляется как список одного или нескольких элементов ELEMENT, содержащийся в подразделе ENTRY.

Список элементов ELEMENT подраздела ENTRY задает условия отбора, соединяемые оператором ИЛИ. Подразделы ENTRY раздела SECTION задают условия отбора, соединяемые оператором И. Следовательно, такая спецификация запроса может, например, использоваться для указания, что политика разрешает предоставить данные ЭМК психиатрам или гинекологам, работающим в конкретной больнице.

Раздел SECTION типа EHR_target используется для указания частей ЭМК пациента, к которым применяется политика. Части ЭМК могут задаваться очень специфичным образом, например, с по-

мощью идентификатора rc_id конкретного тома FOLDER или путем указания списка конкретных компонентов RECORD_COMPONENT (в частности, некоторых из тех, которые передаются в той же самой выписке EHR_EXTRACT). Альтернативой может служить определение частей ЭМК с помощью множества архетипов и/или периода времени. Это позволяет, например, задавать политику, применяемую ко всем результатам микробиологических исследований, полученных с 2003 по 2005 годы. Могут включаться и другие критерии отбора в форме строковых выражений.

Как и в случае спецификации запроса, список элементов ELEMENT подраздела ENTRY задает условия отбора, соединяемые оператором ИЛИ, а подразделы ENTRY раздела SECTION целевых данных (EHR_target) задают условия отбора, соединяемые оператором И.

Раздел SECTION, описывающий правила доступа, используется, чтобы задать разрешения, применяемые к запросам, удовлетворяющим спецификации запроса данных, совпадающей со спецификацией целевых данных. В простейшем случае правило может состоять в разрешении или отказе полного доступа к целевым данным. Однако для обеспечения определенной гибкости подраздел ENTRY, описывающий архетип максимальной категории чувствительности, представляет разрешение доступа в форме целого числа, указывающего максимальную категорию, необходимую для получения доступа. Значения категорий чувствительности описаны в таблице 2. Если указано целое значение 1, то это означает, что к данным частям ЭМК предоставляется полный доступ, а если значение 6 — полный отказ в доступе. В архетипе максимальной категории чувствительности отдельно указываются целые значения категорий, необходимых для доступа к существующим данным ЭМК, для создания новых данных, изменения данных и передачи данных третьей стороне. Такой набор четырех значений разрешает получателю ЭМК, например, иметь право доступа на чтение данных ЭМК без права передачи третьей стороне или читать существующие данные без права их изменения и добавления новых данных к этой части электронной медицинской карты.

Другая часть раздела правил доступа используется для указания, разрешается ли доступ ко всем историческим версиям данных ЭМК или только к текущей (наиболее недавней) версии. Такое указание может требоваться в некоторых политиках доступа для соответствия действующему законодательству по защите данных.

Дополнительные правила могут быть заданы в строковом виде. Если используются такие строковые спецификации, то их однозначная интерпретация людьми и/или компьютерами должна обеспечиваться сторонами, совместно использующими ЭМК.

Общее назначение архетипа, описанного в композиции COMPOSITION, — обеспечить представление базовой информации политики доступа в простой и интероперабельной форме, допускающей включение и передачу более сложных правил. Однако поставщик ЭМК должен быть уверен, что получатель ЭМК способен понять и применить такие дополнительные правила, иначе их включение не принесет никакой пользы.

В разных ведомствах и в разных системах ведения ЭМК уровни структуры ЭМК, на которых задаются и реализуются ограничения доступа, различаются. Ясно, что задание ограничений доступа на очень низком уровне (например, на уровне подразделов ENTRY или даже еще ниже) приведет к тому, что разные классы пользователей будут получать совершенно разную информацию из одной и той же композиции COMPOSITION, что создаст клинические риски и риски управления версиями. Если ограничения доступа указаны в выписке EHR_EXTRACT на более низком уровне, чем способна воспроизвести система, получающая выписку, то этой системе будет трудно правильно выполнить эти ограничения. В таких случаях требуется принимать решение, надо ли минимизировать клинический риск (например, применяя ко всей композиции COMPOSITION политику, эквивалентную наименьшему ограничению на содержание композиции) или же минимизировать возможные юридические последствия (например, применяя ко всей композиции COMPOSITION политику, эквивалентную наивысшему ограничению). Поэтому рекомендуется, чтобы ведомства по возможности санкционировали применение политик на уровне отдельных композиций или их групп, а не на уровне разделов SECTION или подразделов ENTRY.

Необходимо принять во внимание, что такое представление предназначено для передачи информации о политике внутри выписки EHR_EXTRACT и не должно интерпретироваться ни как модель политики в компонентах подсистем безопасности, ни как спецификация политик при передаче из одной подсистемы безопасности в другую.

6.2 Архетип композиции политики доступа

На рисунке 4 показана структура дерева архетипа политик доступа. Отступы вправо означают вложение. Каждый класс компонентов RECORD_COMPONENT показан с использованием следующих обозначений (включая цветовые выделения, хотя они и не требуются для интерпретации рисунка):

- F: xxx в коричневом цвете означает том FOLDER с атрибутом назначения тома xxx;
- C: xxx в красном цвете означает композицию COMPOSITION с атрибутом назначения композиции xxx;
- S: xxx в желтом цвете означает раздел SECTION с атрибутом назначения раздела xxx;
- E: xxx в темно-голубом цвете означает подраздел ENTRY с атрибутом назначения подраздела xxx;
- e: xxx в зеленом цвете означает элемент ELEMENT с атрибутом назначения элемента xxx;
- D_V: XXXX означает значение данных типа XXXX.

Обязательность и кратность каждого узла дерева показаны слева от имени узла.

EHR_EXTRACT							
0..1	**F: Access policies**						
	0..*	**C: Access policy**					
		1..1	**E: Effective time**				
			1..*	**e: time interval**			
					D_V: IVL<TS>		
		0..1	**S: Request specification**				
			0..1	**E: Functional roles**			
				1..*	**e: functional role**		
						D_V: CS_FUNC_ROLE	
			0..1	**E: Functional responsibilities**			
				1..*	**e: functional responsibility**		
						D_V: CV	
			0..1	**E: Structural roles**			
				1..*	**e: structural role**		
						D_V: CV	
			0..1	**E: Clinical settings**			
				1..*	**e: clincial setting**		
						D_V: CS_SETTING	
			0..1	**E: Specialities**			
				1..*	**e: speciality**		
						D_V: CV	
			0..1	**E: Parties**			
				1..*	**e: identified_party**		
						D_V: II	
			0..1	**E: Other requestor characteristics**			
				1..*	**e: EHR requestor description**		
						D_V: TEXT	
		0..1	**S: EHR_target**				
			0..1	**E: Record components**			
				1..*	**e: rc_id**		
						D_V: II	
			0..1	**E: Archetypes**			
				1..*	**e: archetype_id**		
						D_V: II	
			0..1	**E: Time period**			
				1..*	**e: time interval**		
						D_V: IVL<TS>	
			0..1	**E: Other selection criterion**			
				1..*	**e: EHR selection criterion**		
						D_V: TEXT	
		1..1	**S: Access rules**				
			0..1	**E: Maximum sensitivity**			
				1..1	**e: access**		
						D_V: INT	
				1..1	**e: create**		
						D_V: INT	
				1..1	**e: revise**		
						D_V: INT	
				1..1	**e: communicate**		
						D_V: INT	
			1..1				
				E: Version history			
				1..1	**e: all_versions**		
						D_V: BL	
			0..*	**E: Other rules**			
				1..*	**e: access_rule**		
						D_V: TEXT	

Рисунок 4 — Представление архетипа политики доступа в форме диаграммы

6.3 Представление композиции COMPOSITION архетипа политики доступа на языке ADL

Данная спецификация формально определяет архетип политик доступа на языке определения архетипов ADL (Archetype Definition Language), описанном в ИСО 13606-2. Она является формальным представлением модели, показанной на рисунке 4, и логически эквивалентна представлению на языке UML, показанному на рисунке 5.

Для соответствия настоящему стандарту требуется, чтобы в целях передачи информации о политике доступа в выписку EHR_EXTRACT были включены компоненты RECORD_COMPONENT, отвечающие данному архетипу и удовлетворяющие ИСО 13606-1. Применение ADL для представления или передачи этой информации не является необходимым. Он используется в настоящем подразделе как формализм описания архетипа в данном стандарте.

```
archetype
    CEN-EN13606-COMPOSITION.access_policy.v1
concept
    [at0000] -- Политики доступа для выписки из ЭМК, удовлетворяющей стандарту CEN EN13606
description
    original_author = <
        ["name"] = <"Dipak Kalra">
        ["organisation"] = <"gost.e-ecolog.ru                    ">
    >
    other_contributors = <
        ["1"] = <"xxxx">
        ["2"] = <"xxxx">
    >
    lifecycle_state = <"проект">
    archetype_package_uri = <gost.e-ecolog.ru                                    >
    details = <
        ["en"] = <
            language = <"en">
            purpose = <"Передача специфичных ограничений на раскрытие информации, которые должны применяться к компонентам данной выписки из ЭМК">
            keywords = <"контроль доступа", "политика безопасности", "чувствительность", "управление привилегиями", "ролевой контроль доступа">
            use = <"Эта модель предназначена для передачи ограничений доступа, которые должны применяться к будущим запросам доступа к информации данной выписки из ЭМК; обычно тех ограничений, которые накладываются субъектом медицинской помощи">
            misuse = <"Она не предназначена для представления всех политик, использованных для создания данной выписки: тех политик, которые уже были применены поставщиком ЭМК при создании выписки, и других, которые могут не иметь отношения к получателю ЭМК">
            copyright = <"CEN">
            original_resource_uri = <
                ["xxx"] = <gost.e-ecolog.ru                                  >
            >
        >
    >
definition
    COMPOSITION[at0000] matches {
        content cardinality matches {1..*} matches {
            ENTRY[at0001] occurrences matches {1..1} matches {
                data cardinality matches {1..*} matches {
                    ELEMENT[at0002] matches {
                        value matches {
                            IVL<TS> matches {*}
                        }
                    }
                }
            }
```

```
SECTION[at0003] occurrences matches {0..1} matches {
    items cardinality matches {0..*} matches {
        ENTRY[at0004] occurrences matches {1..1} matches {
            data cardinality matches {1..*} matches {
                ELEMENT[at0005] matches {
                    value matches {
                        CS_FUNC_ROLE matches {*}
                    }
                }
            }
        }
        ENTRY[at0006] occurrences matches {1..1} matches {
            data cardinality matches {1..*} matches {
                ELEMENT[at0007] matches {
                    value matches {
                        CV matches {*}
                    }
                }
            }
        }
        ENTRY[at0008] occurrences matches {1..1} matches {
            data cardinality matches {1..*} matches {
                ELEMENT[at0009] matches {
                    value matches {
                        CS_SETTING matches {*}
                    }
                }
            }
        }
        ENTRY[at0010] occurrences matches {1..1} matches {
            data cardinality matches {1..*} matches {
                ELEMENT[at0011] matches {
                    value matches {
                        CV matches {*}
                    }
                }
            }
        }
        ENTRY[at0012] occurrences matches {1..1} matches {
            data cardinality matches {1..*} matches {
                ELEMENT[at0013] matches {
                    value matches {
                        II matches {*}
                    }
                }
            }
        }
        ENTRY[at0014] occurrences matches {1..1} matches {
            data cardinality matches {1..*} matches {
                ELEMENT[at0015] matches {
                    value matches {
                        TEXT matches {*}
                    }
                }
            }
        }
    }
}
```

```
SECTION[at0016] occurrences matches {0..1} matches {
    items cardinality matches {0..*} matches {
        ENTRY[at0017] occurrences matches {1..1} matches {
            data cardinality matches {1..*} matches {
                ELEMENT[at0018] matches {
                    value matches {
                        CS_FUNC_ROLE matches {*}
                    }
                }
            }
        }
        ENTRY[at0019] occurrences matches {1..1} matches {
            data cardinality matches {1..*} matches {
                ELEMENT[at0020] matches {
                    value matches {
                        CV matches {*}
                    }
                }
            }
        }
        ENTRY[at0021] occurrences matches {1..1} matches {
            data cardinality matches {1..*} matches {
                ELEMENT[at0022] matches {
                    value matches {
                        CS_SETTING matches {*}
                    }
                }
            }
        }
        ENTRY[at0023] occurrences matches {1..1} matches {
            data cardinality matches {1..*} matches {
                ELEMENT[at0024] matches {
                    value matches {
                        CV matches {*}
                    }
                }
            }
        }
    }
}
SECTION[at0025] occurrences matches {1..1} matches {
    items cardinality matches {0..*} matches {
        ENTRY[at0026] occurrences matches {1..1} matches {
            data cardinality matches {1..*} matches {
                ELEMENT[at0027] matches {
                    value matches {
                        INT matches {*}
                    }
                }
                ELEMENT[at0028] matches {
                    value matches {
                        INT matches {*}
                    }
                }
                ELEMENT[at0029] matches {
                    value matches {
                        INT matches {*}
                    }
                }
```

```
                    ELEMENT[at0030] matches {
                        value matches {
                            INT matches {*}
                        }
                    }
                }
            }
            ENTRY[at0031] occurrences matches {1..1} matches {
                data cardinality matches {1..*} matches {
                    ELEMENT[at0032] matches {
                        value matches {
                            BL matches {*}
                        }
                    }
                }
            }
            ENTRY[at0033] occurrences matches {1..1} matches {
                data cardinality matches {1..*} matches {
                    ELEMENT[at0034] matches {
                        value matches {
                            TEXT matches {*}
                        }
                    }
                }
            }
        }
    }
}
ontology
    primary_language = <"en">
    languages_available = <"en">
    term_definitions = <
        ["en"] = <
            items = <
                ["at0000"] = <
                    description = <"Политики доступа для выписки из ЭМК, удовлетворяющей стандарту
CEN EN13606">
                    text = <"Политики доступа">
                >
                ["at0001"] = <
                    description = <"Сроки действия данной политики">
                    text = <"срок действия">
                >
                ["at0002"] = <
                    description = <"Конкретный срок, когда данная политика должна действовать">
                    text = <"временной интервал">
                >
                ["at0003"] = <
                    description = <"Совокупность характеристик, определяющая тип будущих запросов
ЭМК, для которых должна использоваться данная политика">
                    text = <"спецификация запроса">
                >
                ["at0004"] = <
                    description = <"Список функциональных ролей лица, запрашивающего ЭМК, к которым
применяется данная политика">
                    text = <"функциональные роли">
                >
```

```
["at0005"] = <
    description = <"Функциональная роль, определенная в 6.2 настоящего стандарта">
    text = <"функциональная роль">
>
["at0006"] = <
    description = <"Список структурных ролей лица, запрашивающего ЭМК, к которым применяется данная политика">
    text = <"структурные роли">
>
["at0007"] = <
    description = <"Структурная роль, в будущем должна браться из словаря, определенного ТК 215 ИСО">
    text = <"структурная роль">
>
["at0008"] = <
    description = <"Список условий оказания медицинской помощи, для которых применяется данная политика">
    text = <"условия оказания медицинской помощи">
>
["at0009"] = <
    description = <"Конкретные условия оказания медицинской помощи, взятые из списка, предложенного в настоящем стандарте">
    text = <"условия оказания медицинской помощи">
>
["at0010"] = <
    description = <"Список медицинских специальностей в организации, запрашивающей ЭМК, на которые распространяется настоящая политика">
    text = <"специальности">
>
["at0011"] = <
    description = <"Любое кодирование представления медицинской специальности, на которую распространяется данная политика: местные правила должны определить, какой список терминов должен быть использован для обеспечения интероперабельности">
    text = <"специальность">
>
["at0012"] = <
    description = <"Список лиц, на которые распространяется данная политика">
    text = <"стороны">
>
["at0013"] = <
    description = <"Специфичная идентифицированная сторона">
    text = <"идентифицированная сторона">
>
["at0014"] = <
    description = <"Совокупность дополнительных дескрипторов лица, запрашивающего ЭМК, которые либо определены местными правилами, либо должны соответствовать региональным или национальным правилам или законам">
    text = <"другие атрибуты лица, запрашивающего ЭМК">
>
["at0015"] = <
    description = <"Специфичный дескриптор профиля лица, запрашивающего ЭМК, к которому применяется данная политика">
    text = <"дескриптор лица, запрашивающего ЭМК">
>
```

```
        ["at0016"] = <
            description = <"Список характеристик, определяющий части электронной медицинской карты данного субъекта медицинской помощи, на которые должна распространяться данная политика">
            text = <"целевые части ЭМК">
        >
        ["at0017"] = <
            description = <"Список специфичных экземпляров компонентов ЭМК, к которым применяется данная политика">
            text = <"компоненты ЭМК">
        >
        ["at0018"] = <
            description = <"Конкретный компонент ЭМК, к которому применяется данная политика">
            text = <"rc_id">
        >
        ["at0019"] = <
            description = <"Список архетипов, к которым применяется данная политика">
            text = <"архетипы">
        >
        ["at0020"] = <
            description = <"Идентификатор архетипа: эта политика применяется ко всем экземплярам компонентов ЭМК, соответствующих части данного архетипа">
            text = <"archetype_id">
        >
        ["at0021"] = <
            description = <"Список временных интервалов: эта политика применяется ко всем экземплярам компонентов ЭМК, записанных в базу данных в момент времени, попадающий в любой из этих интервалов">
            text = <"временные интервалы">
        >
        ["at0022"] = <
            description = <"Конкретный временной интервал: эта политика применяется ко всем экземплярам компонентов ЭМК, записанных в базу данных в момент времени данного интервала">
            text = <"временной интервал">
        >
        ["at0023"] = <
            description = <"Список дополнительных дескрипторов части электронной медицинской карты данного субъекта, к которым применяется данная политика">
            text = <"другие критерии отбора">
        >
        ["at0024"] = <
            description = <"Специфичный дескриптор компонента ЭМК, к которому применяется данная политика">
            text = <"критерии отбора данных ЭМК">
        >
        ["at0025"] = <
            description = <"Список разрешений (правил), диктуемых данной политикой">
            text = <"правила доступа">
        >
        ["at0026"] = <
            description = <"Максимальная категория чувствительности целевого компонента ЭМК, которой согласно данной политике должно быть наделено профилированное лицо, запрашивающее ЭМК, чтобы иметь возможность выполнить конкретные функции системы ведения ЭМК, определенные элементами настоящего подраздела. Категория чувствительности задается в соответствии с 6.1 настоящего стандарта">
            text = <"максимальная категория чувствительности">
        >
```

```
            ["at0027"] = <
                description = <"Максимальная категория чувствительности, которую надо иметь для доступа к данным ЭМК">
                text = <"доступ">
            >
            ["at0028"] = <
                description = <"Максимальная категория чувствительности, которую надо иметь для отправки в ЭМК новых компонентов этого типа">
                text = <"создание">
            >
            ["at0029"] = <
                description = <"Максимальная категория чувствительности компонента ЭМК, которую надо иметь запрашивающему лицу для изменения или логического удаления данных ЭМК">
                text = <"изменение">
            >
            ["at0030"] = <
                description = <"<"Максимальная категория чувствительности компонента ЭМК, которую надо иметь запрашивающему лицу для его передачи третьей стороне">
                text = <"передача">
            >
            ["at0031"] = <
                description = <"Инструкция данной политики в части доступа к прежним версиям данных ЭМК">
                text = <"история версий">
            >
            ["at0032"] = <
                description = <"Булевское значение, указывающее, может ли данный класс запрашивающих лиц иметь доступ к прежним версиям измененного компонента ЭМК, если они имеют доступ к измененному компоненту">
                text = <"все версии">
            >
            ["at0033"] = <
                description = <"Список дополнительных правил, которые могут быть заданы на местном уровне и/или требуются для соответствия региональным или национальным правилам или законам">
                text = <"другие правила">
            >
            ["at0034"] = <
                description = <"Специфичное местное правило доступа">
                text = <"правило доступа">
            >
            >
        >
    >
:
```

6.4 Представление архетипа композиции политики доступа на языке UML

Диаграмма классов на языке UML, показанная на рисунке 5, логически эквивалентна представлению архетипа на языке ADL, приведенному в 6.3. Она включена в настоящий стандарт для совместимости с передачей информации политики доступа в соответствии с ИСО/ТС 22600.

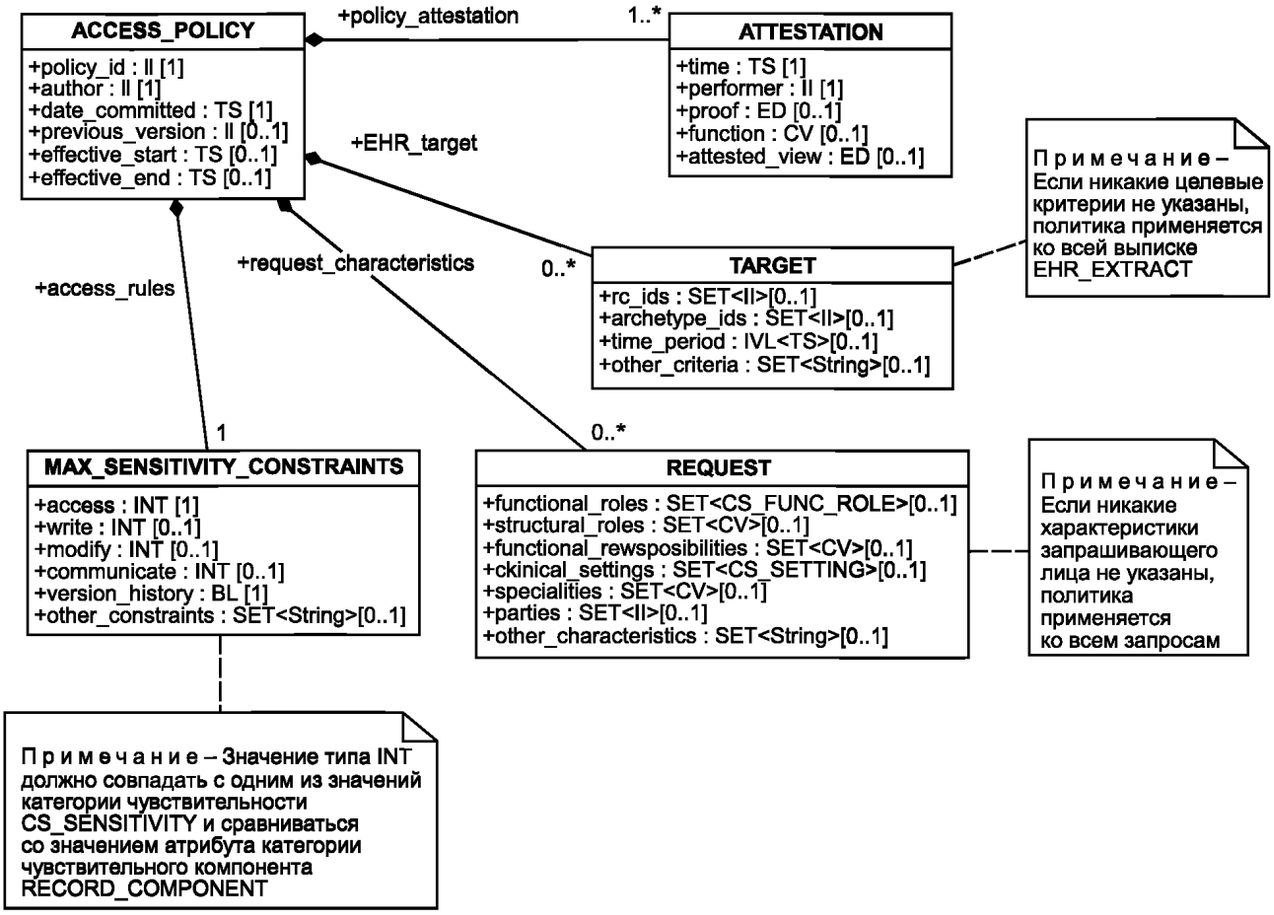


Рисунок 5 — Представление модели политики доступа на языке UML

7 Представление информации журнала аудита — модель объекта EHR_AUDIT_LOG_EXTRACT

Чтобы передача журнала аудита соответствовала требованиям настоящего стандарта, необходимо использовать информационную модель журнала, показанную на рисунке 6. Определение классов и атрибутов приведено под рисунком.

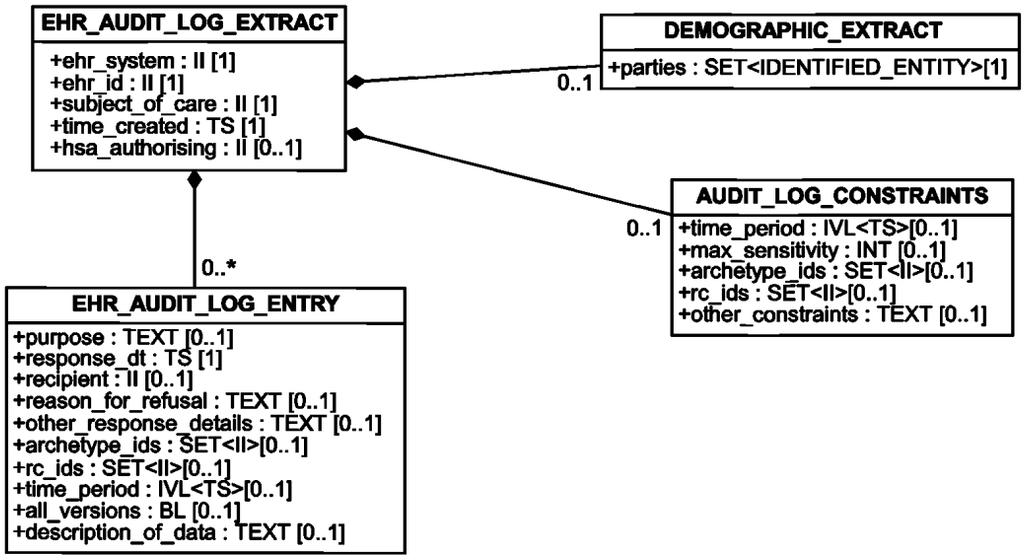


Рисунок 6 — Представление модели выдержки из журнала аудита ЭМК на языке UML

Класс EHR_AUDIT_LOG_EXTRACT

Согласно настоящему стандарту этот класс является корневым и описывает данные журнала аудита ЭМК в форме, предназначенной для передачи.

Атрибут ehr_system: II [1]

Уникальный идентификатор системы ведения ЭМК, хранящей электронную медицинскую карту, к которой был осуществлен доступ.

Атрибут ehr_id: II [1]

Уникальный идентификатор электронной медицинской карты, к которой был осуществлен доступ.

Атрибут subject_of_care: II [1]

Уникальный идентификатор субъекта медицинской помощи, к которому относится эта ЭМК.

Атрибут time_created: TS [1]

Дата и время выборки данной информации из системы ведения журнала аудита.

Атрибут hca_authorising: II [0.1]

Идентификатор стороны, которая авторизовала создание и передачу данной выдержки из журнала аудита.

Класс DEMOGRAPHIC_EXTRACT [0..1]

Атрибут parties: SET<IDENTIFIED_ENTITY>

Данный класс идентичен классу с соответствующим именем, определенному в эталонной информационной модели ЭМК в ИСО 13606-1. Этот же самый пакет должен использоваться для включения базовой описательной информации обо всех сторонах, идентифицированных в данной выдержке из журнала аудита (субъекте медицинской помощи, посредниках в системе здравоохранения, организациях, устройствах и т. д.).

Класс AUDIT_LOG_CONSTRAINTS [0..1]

Этот класс определяет фильтр, примененный в ответ на запрос при генерации данной выдержки из журнала аудита.

Атрибут time_period: IVL<TS> [0..1]

Период времени, охватываемый данной выдержкой из журнала аудита.

Атрибут max_sensitivity: Integer [0..1]

Максимальная категория чувствительности компонентов RECORD_COMPONENT, доступ к которым зарегистрирован в данной выдержке из журнала аудита.

Атрибут archetype_ids: SET<II> [0..1]

Множество архетипов, которыми ограничена данная выдержка из журнала аудита.

Атрибут rc_ids: SET<II> [0..1]

Множество компонентов RECORD_COMPONENT, которыми ограничена данная выдержка из журнала аудита.

Атрибут other_constraints: TEXT [0..1]

Любые другие ограничения содержания данной выдержки из журнала аудита. Поскольку этот атрибут имеет текстовый тип данных, эти дополнительные ограничения могут оказаться непригодными для автоматической обработки.

Класс EHR_AUDIT_LOG_ENTRY [0..*]

Класс EHR_AUDIT_LOG_EXTRACT содержит множество записей EHR_AUDIT_LOG_ENTRY, каждая из которых содержит сведения об одном акте доступа к данной электронной медицинской карте в системе ведения ЭМК. Запись журнала аудита содержит информацию о данных ЭМК, к которым был предоставлен доступ, кому и когда он был предоставлен.

Атрибут purpose: TEXT [0..1]

Описание обоснования данного запроса ЭМК.

Атрибут response_dt: TS [1]

Дата и время предоставления ответа системой ведения ЭМК.

Атрибут recipient: II [0..1]

Сторона, которой переданы данные ЭМК. Ею может быть, а может и не быть лицо, названное получателем в запросе.

Атрибут reason_for_refusal: TEXT [0..1]

Описание причины, по которой запрос был отклонен или частично удовлетворен. Этому атрибуту присвоен текстовый тип данных, поскольку формального справочника кодов пока нет.

Атрибут other_response_details: TEXT [0..1]

Этот атрибут может использоваться для представления любых других деталей запроса, например, описания любых событий, в связи с которыми инициирован доступ, или факторов, которые вызвали передачу данных ЭМК без запроса с чьей-либо стороны.

Атрибут archetype_ids: SET<II> [0..1]

Множество архетипов, включенных в данную выписку EHR_EXTRACT.

Атрибут rc_ids: SET<II> [0..1]

Множество компонентов RECORD_COMPONENT, включенных в данную выписку EHR_EXTRACT.

Атрибут time_period: IVL<TS> [0..1]

Период времени, охватываемый данной выпиской EHR_EXTRACT, если она была получена из ЭМК с помощью фильтрации по временному периоду.

Атрибут all_versions: BL [0..1]

Этот атрибут указывает, все ли версии включены в данную EHR_EXTRACT.

Атрибут description_of_data: TEXT [0..1]

Этот атрибут содержит любые другие детали описания выписки из электронной медицинской карты или ограничений, примененных при ее создании.

Приложение А
(справочное)

Пример контроля доступа

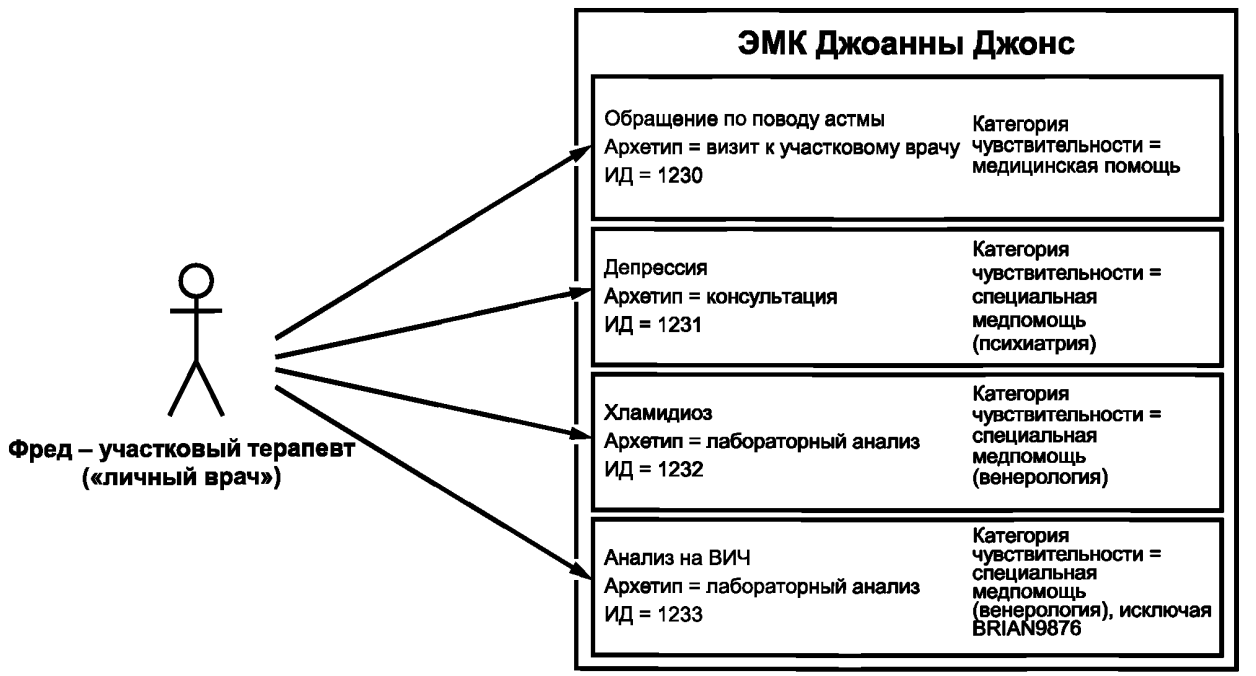
Приведенные ниже диаграммы демонстрируют способ применения относительно простых политик для обеспечения достаточно гибких возможностей управления доступом к данным одной ЭМК.

Предположим, что электронная медицинская карта Джоанны Джонс содержит четыре композиции:

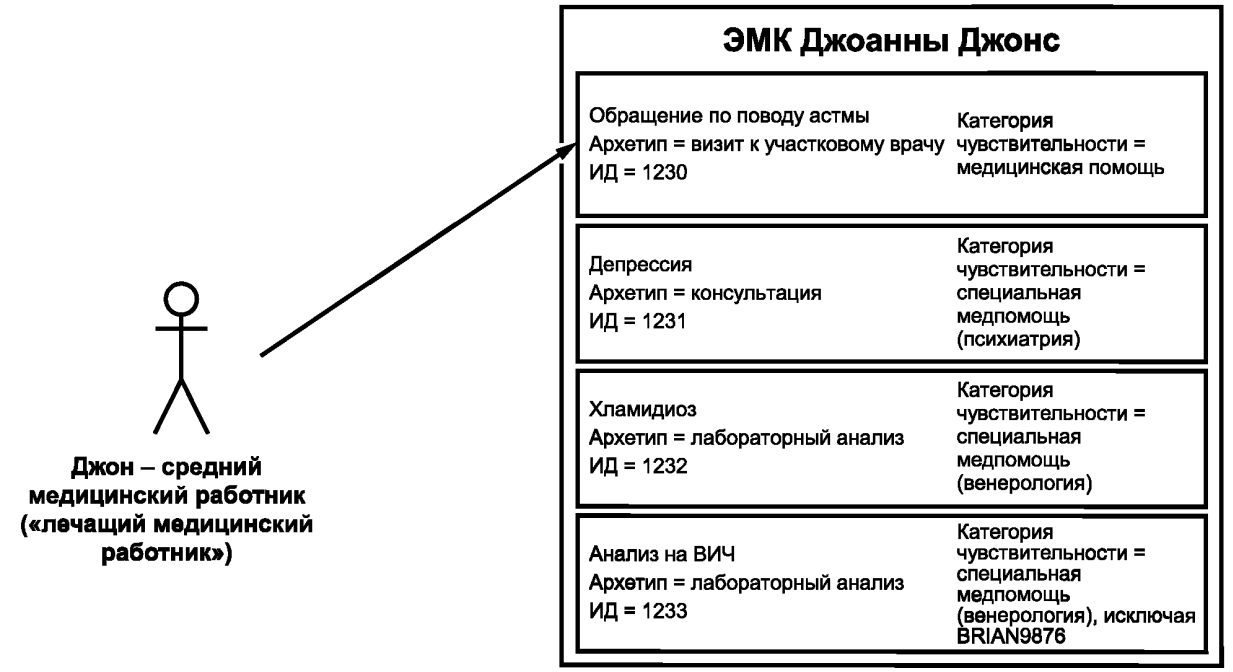
- обращение по поводу астмы к своему участковому терапевту;
- консультация психиатра в поликлиническом отделении стационара по поводу депрессии;
- результат лабораторного анализа в кожно-венерологическом диспансере, подтверждающий хламидиоз;
- результат анализа на ВИЧ.

Каждая из этих композиций имеет определенную категорию чувствительности (в соответствии с 5.1). Композиция анализа на ВИЧ содержит также ссылку на политику, запрещающую доступ названной стороны к этой композиции.

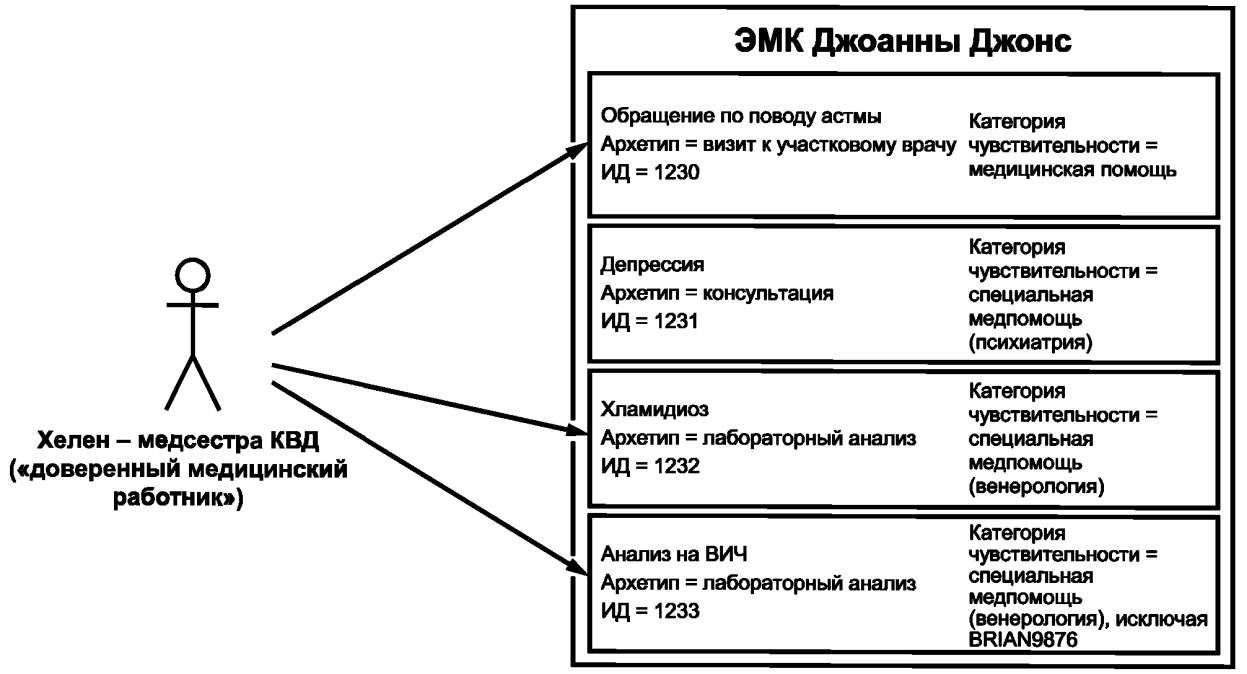
Фред — участковый врач Джоанны; он может иметь доступ к ее ЭМК с функциональной ролью личного врача. Ему разрешен доступ ко всем четырем композициям.



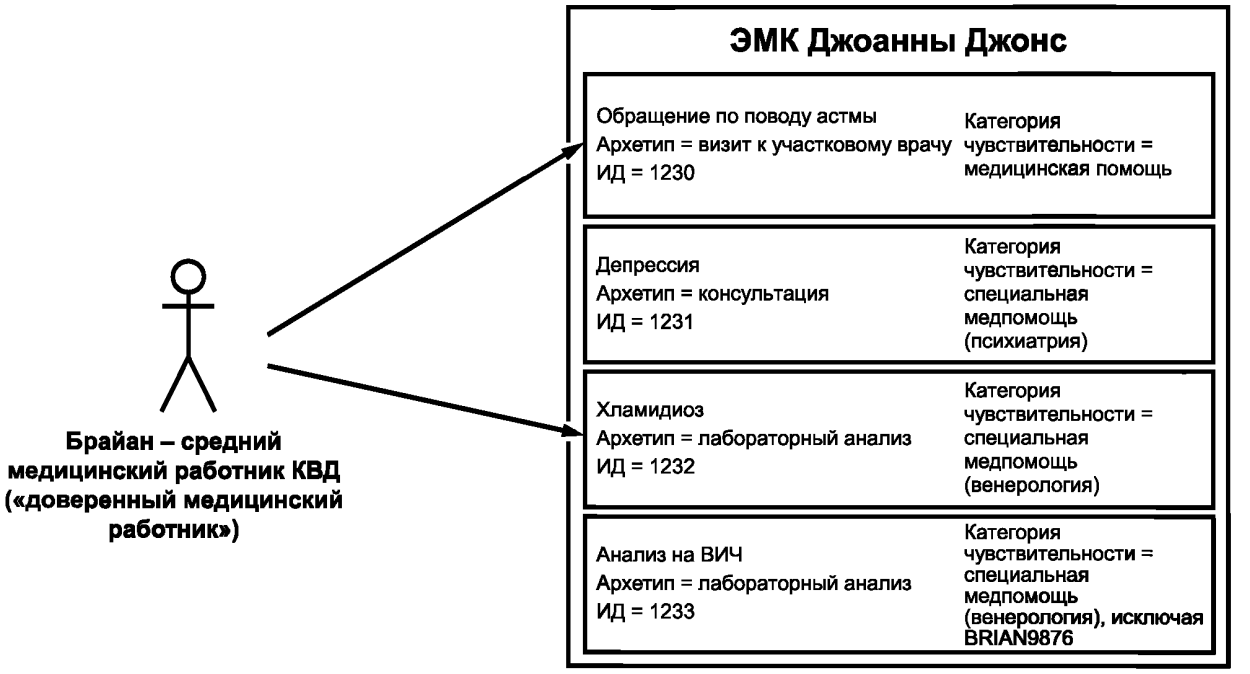
Джон — средний медицинский работник на том же самом терапевтическом участке. Его функциональная роль — лечащий медицинский работник. Поэтому он может получить доступ только к информации об обращении по поводу астмы.



Хелен — медицинская сестра в кожно-венерологическом диспансере. Она может иметь роль доверенного медицинского работника в клинических условиях кожно-венерологического диспансера. Поэтому она может видеть три композиции ЭМК Джоанны, то есть информацию об обращении по поводу астмы и результаты анализов (на хламидиоз и на ВИЧ).



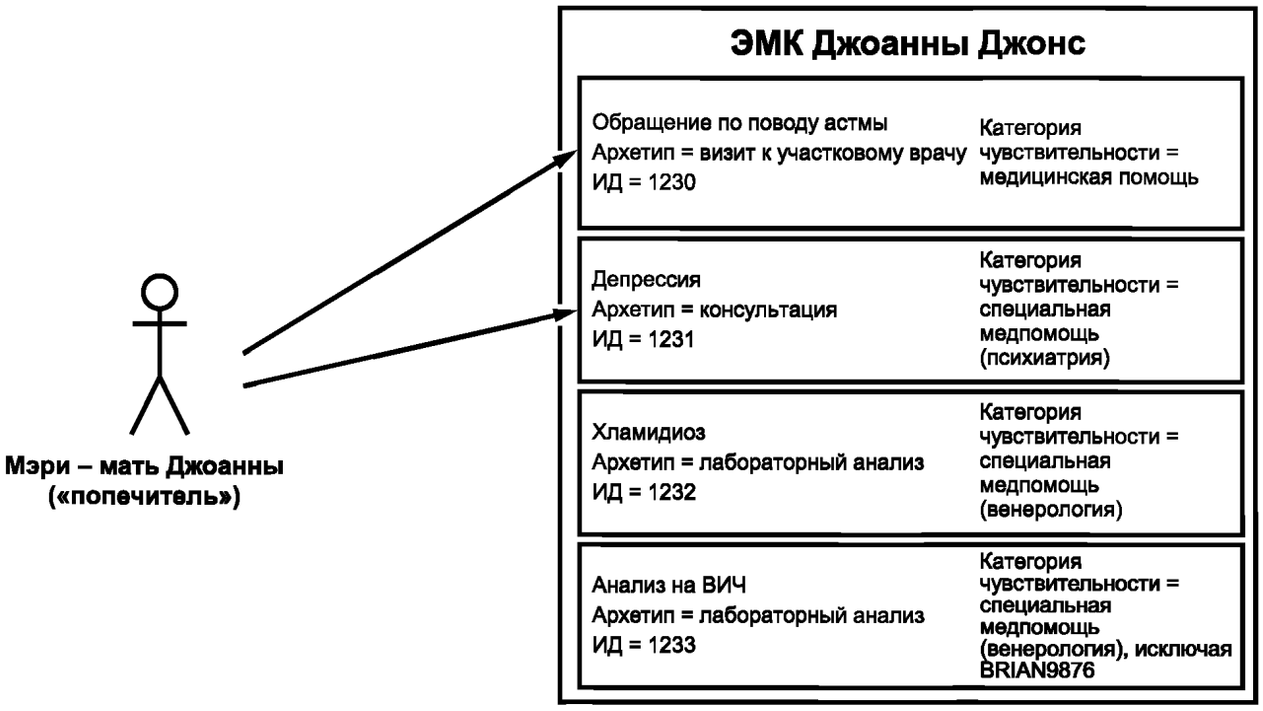
Брайан работает в том же диспансере, что и Хелен, и в обычном случае мог бы иметь доступ к той же информации, что и она. Однако он явным образом исключен из круга лиц, которым доступен результат анализа на ВИЧ, и поэтому может видеть только две композиции электронной медицинской карты Джоанны.



Джоанне только 15 лет, и ее беспокоит, что ее мать как законный представитель имеет юридические права доступа к ее ЭМК. Ей бы не хотелось, чтобы мать знала о ее сексуальной активности, о которой можно было бы легко догадаться, видя результаты анализов на хламидиоз и ВИЧ или просто зная об их существовании. Поэтому Джоанна предложила политику доступа, которая применяется к ЭМК в целом и запрещает родителям иметь доступ к любым результатам лабораторных анализов. Такое ограничение распространяется и на результаты будущих анализов, например, если участковый врач или диспансер направят ее на микробиологические анализы.

Можно ли Джоанне разрешить такую политику или нет, и с чьей санкции — сложный этический вопрос. Национальные законодательства могут иметь разные правила на этот счет, но такая политика в принципе может быть дозволена, если будет сочтено, что Джоанна достигла достаточной зрелости и компетентности, или же факт постановки на учет в кожно-венерологическом диспансере будет давать такие права автоматически.

Цель настоящего примера — показать, как общая политика доступа к ЭМК может применяться для решения подобных задач.



Следует иметь в виду, что такая политика сама по себе означает, что Джоанне есть что скрывать, и поэтому доступ к политике также должен быть ограничен, чтобы мать не знала о ее существовании. Этот пример также иллюстрирует необходимость такого способа отказа запроса на доступ к ЭМК (по причине недостаточных прав доступа), но при этом отказ не может свидетельствовать о том, что какие-то данные скрываются.

Приложение В
(справочное)

Связь со стандартом ENV 13606-3:2000

Как уже было сказано во введении к настоящему стандарту, правила распространения, представленные в стандарте ENV 13606-3:2000, были изменены по следующим причинам:

- некоторые аспекты спецификации стандарта ENV 13606-3:2000, например WHY (цель требования передачи ЭМК), определены с помощью текстовых атрибутов без формализованного словаря, что препятствует достижению интероперабельности;
- общая базовая структура предусматривала гораздо больше деталей контроля доступа, чем реализовано в большинстве современных систем ведения ЭМК, и ее реализация была бы одновременно и дорогой, и трудной;
- она потребовала бы от медицинских работников значительных дополнительных усилий по заполнению экземпляров правил в процессе оперативного ввода данных в ЭМК;
- во многих компьютеризованных системах здравоохранения принимались и принимаются общие меры безопасности, и добавление к ним средств, специфичных для ЭМК, рассматривалось бы как необоснованное.

Известно, что некоторые разработчики использовали этот предварительный стандарт в качестве основы для конструирования политик доступа к ЭМК. Однако рабочая группа по разработке настоящего стандарта не нашла каких-либо сведений о масштабной демонстрации интероперабельности правил распространения политик при обмене данными между информационными системами разных производителей. В таблице В.1 перечислены базовые информационные компоненты (классы и атрибуты) модели правил распространения в том виде, как они были опубликованы в 2000 году, и указаны причины, по которым эти компоненты не были включены в исходном виде в настоящий стандарт, или даны способы их представления в модели политики, определенной в разделе 6.

Таблица В.1 — Информационные компоненты (классы и атрибуты) модели правил распространения, опубликованные в 2000 году

Исходные атрибуты правил распространения		Соответствие модели политики, определенной в разделе 6	Примечание
Категория	Атрибут		
DR reference (ссылка на правила распространения)			Теперь этот класс принципиально соответствует компоненту RECORD_COMPONENT, содержащему политику доступа по ссылке
	Distribution rule unique identifier (уникальный идентификатор правила распространения)	policy_id	
	Applied date and time (дата и время записи)	Момент записи в базу данных компонента RECORD_ COMPONENT	
	Applied by (записавший субъект)	Субъект, инициировавший запись компонента RECORD_ COMPONENT в базу данных	
	Valid from (дата начала действия)	Дата, начиная с которой должна действовать данная политика доступа	
	Valid to (дата прекращения действия)	Дата завершения действия данной политики доступа	
	Negation statement (объявление отрицания)	(Отсутствует)	В разделе SECTION правил доступа будет определено, является ли данная декларация политики разрешением или отказом

Продолжение таблицы В.1

Исходные атрибуты правил распространения		Соответствие модели политики, определенной в разделе 6	Примечание
Категория	Атрибут		
	Basic distribution rule (основное правило распространения)	(Отсутствует)	Между базовыми и небазовыми правилами теперь нет различия
	Invalidated by (перезаписавший субъект)	Субъект, инициировавший запись компонента RECORD_ COMPONENT в базу данных	Представлен с помощью нормального процесса создания версий компонентов RECORD_ COMPONENT
	Country of application (страна применения)	(Отсутствует)	См. комментарий о стране, приведенный ниже раздела WHERE
	Consent demonstration reference	Аттестация политики доступа	Представлен с помощью нормального процесса аттестации RECORD_COMPONENT
Distribution rule (правило распространения)			
	Distribution rule unique identifier (уникальный идентификатор правила распространения)	Идентификатор rc_id политики доступа	
	Access type (тип доступа)	Максимальная категория чувствительности элементов: доступ, создание, изменение, передача	
	Apply DR access (применяется к доступу к правилу распространения)	(Отсутствует)	Если политики доступа передаются как композиции COMPOSITION, то для них тоже могут быть заданы ограничения на доступ, создание, изменение, передачу. Однако вряд ли политики доступа к политикам доступа будут часто передаваться в интероперабельной форме в выписке из ЭМК
	Healthcare agent in context (субъект здравоохранения в контексте)	Автор композиции COMPOSITION, описывающей политику доступа	
WHO (КТО)			
	Profession (профессия)	Структурные роли	В 2000 году не был определен или указан справочник допустимых значений, что не давало возможности обеспечить адекватный уровень интероперабельности. Переименование в «структурную роль» позволяет воспользоваться справочником, определенным в ИСО/ТС 21298
	Specialization (специализация)	Специальности	
	Healthcare agent (субъект здравоохранения)	Стороны	Изменен, чтобы использовать пакет демографических данных, определенный в ИСО 13606-1. Тип данных заменен на II
	Engaged in care (вовлечен в медицинскую помощь)	(См. функциональную роль)	Перенесен в раздел WHY (см. ниже)

Продолжение таблицы В.1

Исходные атрибуты правил распространения		Соответствие модели политики, определенной в разделе 6	Примечание
Категория	Атрибут		
WHEN (КОГДА)			Интервалы времени доступа, разрешенные медицинскому персоналу, трудно определить точно, разве что ретроспективно. Несколько эпизодов оказания медицинской помощи может проходить параллельно и пересекаться по времени. Продолжение доступа к ЭМК может требоваться в течение некоторого времени после завершения эпизода, чтобы зарегистрировать осложнения или дать ответы на запрос следующих поставщиков медицинской помощи. Поэтому фасет времени WHEN был удален. Параметр срока действительности позволяет задать интервал времени, когда доступ разрешен
	Episode of care (эпизод лечения)	(Отсутствует)	См.выше
	Episode reference (ссылка на эпизод лечения)	(Отсутствует)	См.выше
	Episode description (описание эпизода лечения)	(Отсутствует)	См.выше
WHERE (ГДЕ)			Поскольку содержание ЭМК постепенно интернационализируется (например, может содержать композиции, созданные в разных странах) и доступ к нему тоже может требоваться в разных странах, то предполагается, что разрешение или отказ в доступе, специфичные для конкретной страны, не могут быть указаны как свойство одной или всех ЭМК. Существующие национальные правила и законы могут быть представлены с помощью критериев, определенных в разделе 6, а не путем простого указания страны или географической области. В частности, явное информированное согласие на перемещение данных внутри Европейского союза не требуется, если такое перемещение совместимо с целями доступа к данным (например, оказание медицинской помощи). Поэтому эта характеристика исключена
	Country specificity (специфичность для страны)	(Отсутствует)	См. выше
	Legal requirement (требование законодательства)	(Отсутствует)	См. выше

Продолжение таблицы В.1

Исходные атрибуты правил распространения		Соответствие модели политики, определенной в разделе 6	Примечание
Категория	Атрибут		
		Условия оказания медицинской помощи	Этот атрибут добавлен для указания, что доступ разрешен только для определенных условий оказания медицинской помощи (типов учреждений здравоохранения или их подразделений), например, только для кожно-венерологического диспансера. Такие ограничения нередко накладываются национальным законодательством. В будущем ИСО определит для значений этого атрибута новый справочник
WHY (ПОЧЕМУ)			Основная сложность редактирования этой части правил распространения состояла в поиске универсального и согласованного с другими приложениями справочника целей доступа, который послужил бы удобной и масштабируемой основой для деления электронной медицинской карты на части из соображений безопасности. Имеющийся опыт показывает, что в данном контексте будет работать только самая простейшая категоризация. В противном случае возникают сложные риски отказа во вполне законном доступе медицинскому персоналу, чья медицинская помощь не была предусмотрена в момент отправки информации электронной медицинской карты в базу данных
	Healthcare process code (код процесса медицинской помощи)	(Отсутствует)	Атрибут удален, поскольку в предварительном стандарте не был определен конкретный справочник и точность определения этого атрибута не обеспечивала интероперабельного принятия решений о доступе. Вместо него можно использовать функциональную ответственность
	Healthcare process text (название процесса медицинской помощи)	(Отсутствует)	См. выше
	Sensitivity class (категория чувствительности)		Теперь он включен в новую категорию "ЧТО" ("WHAT") (см. ниже)
	Purpose of use (цель применения)		
	Purpose of use code (код цели применения)	(Отсутствует)	Атрибут удален, поскольку в предварительном стандарте не был определен конкретный справочник и точность определения этого атрибута не обеспечивала интероперабельного принятия решений о доступе. Вместо него можно использовать функциональную ответственность

Продолжение таблицы В.1

Исходные атрибуты правил распространения		Соответствие модели политики, определенной в разделе 6	Примечание
Категория	Атрибут		
	Purpose of use text (название цели применения)	(Отсутствует)	См. выше
	Specific purpose of use (специфичная цель применения)	Функциональная ответственность	Этот атрибут имеет тип данных CV, но для обеспечения интероперабельности сообщества разработчиков должны согласовать конкретные термины или отображение на универсальную терминологию
	Activity (деятельность)	(Отсутствует)	Атрибут удален, поскольку в предварительном стандарте не был определен конкретный справочник и точность определения этого атрибута не обеспечивала интероперабельного принятия решений о доступе. Вместо него можно использовать функциональную ответственность
	Subject of care (субъект медицинской помощи)	Стороны	Субъект медицинской помощи идентифицируется в пакете DEMOGRAPHIC_EXTRACT, определенном в ИСО 13606-1
	Healthcare party role (роль стороны, оказывающей медицинскую помощь)		
	Healthcare party code (код роли стороны, оказывающей медицинскую помощь)	Функциональная роль	
	Healthcare party text (название роли стороны, оказывающей медицинскую помощь)	Функциональная роль	
HOW (КАК)			В настоящее время принято считать, что политики безопасности этого типа, рассмотренные в стандарте ENV 13606-3 (как часть раздела HOW), должны определяться организациями, службами здравоохранения или региональными органами управления здравоохранением и не должны оговариваться на уровне отдельной ЭМК. Также считается, что задание ограничений на технологии доступа является гораздо более сложной задачей, чем те, которые можно решить с помощью первоначально определенных атрибутов этого раздела. Поэтому раздел HOW был полностью удален
	Access method (метод доступа)		

Продолжение таблицы В.1

Исходные атрибуты правил распространения		Соответствие модели политики, определенной в разделе 6	Примечание
Категория	Атрибут		
	Security policy (политика безопасности)		
	Security policy text (текст политики безопасности)		
	Signed (подписан)		
	Encrypted distribution (шифрованное распространение)		
	Encrypted storage (шифрованное хранение)		
	Operating system security rating (класс защиты операционной системы)		
	Physical security rating (класс физической защиты)		
	Software security rating (класс защиты программного обеспечения)		
	Consent required (требуется информированное согласие)		Теперь считается достаточным, если субъект медицинской помощи может аттестовать политику доступа (и тем самым согласиться с ее определением) и аттестовать компоненты RECORD_COMPONENT, которые ссылаются на заданную политику (и тем самым согласиться с ее применением к этим частям ЭМК). Требование информированного согласия пациента во время исполнения программного обеспечения может быть обеспечено путем ограничения доступа пациента к данным. Поэтому этот класс был удален
	Healthcare party (сторона, оказывающая медицинскую помощь)		
	Consent method code (код метода получения информированного согласия)		
	Consent method text (название метода получения информированного согласия)		
	Healthcare party role (роль стороны, оказывающей медицинскую помощь)		
	Healthcare party code (код роли стороны, оказывающей медицинскую помощь)		

Окончание таблицы В.1

Исходные атрибуты правил распространения		Соответствие модели политики, определенной в разделе 6	Примечание
Категория	Атрибут		
	Healthcare party text (название роли стороны, оказывающей медицинскую помощь)		
WHAT (ЧТО)			Исходные правила распространения подразумевали, что на каждое правило должна быть ссылка из одного или нескольких архитектурных компонентов ЭМК. Хотя это могло бы позволить задавать детальные политики доступа, необходима также масштабируемая возможность определения некоторых политик на уровне ЭМК в целом или на уровне отдельных частей ЭМК по ссылке (например, правило могло бы применяться в соответствии с некоторым алгоритмом). Для ее реализации потребовалось добавление к спецификации категории WHAT. Этот подход позволяет также применять объявления контроля доступа к совокупности компонентов, которые уже существуют в ЭМК — БЕЗ НЕОБХОДИМОСТИ ПЕРЕСМОТРА КАТЕГОРИИ КАЖДОГО ОТДЕЛЬНОГО КОМПОНЕНТА ПРИ ДОБАВЛЕНИИ ЕГО В ЭТУ СОВОКУПНОСТЬ. Этот подход значительно облегчает эксплуатацию крупных политик, которые могут регулярно пересматриваться для отражения воли пациента
		Компоненты ЭМК	Политика доступа применяется к одному или нескольким специфичным компонентам RECORD_COMPONENT (например, к конкретному тому FOLDER)
		Архетипы	Этот атрибут позволяет ассоциировать объявления контроля доступа с классами данных ЭМК и тем самым автоматически распространять их на любые новые данные, добавленные к данному архетипу
		Временной период	Этот атрибут позволяет применять политику к сегментам ЭМК в зависимости от времени их действия (в отличие от срока действия самой политики)

Приложение ДА
(справочное)

Сведения о соответствии ссылочных международных стандартов и документов ссылочным национальным стандартам Российской Федерации

Таблица ДА.1

Обозначение ссылочного международного стандарта, документа	Степень соответствия	Обозначение и наименование соответствующего национального стандарта
ИСО 13606-1:2008	—	ГОСТ Р ИСО 13606-1—2011 «Информатизация здоровья. Передача электронных медицинских карт. Часть 1. Базовая модель»
ИСО 13606-2:2008	—	*
ИСО 13606-5:2010	—	*
ИСО/ТС 21298:2008	—	
ИСО/МЭК 27002:2005	—	*
ИСО 27799:2008	—	*
ИСО/ТС 22600-1:2006	IDT	ГОСТ Р ИСО/ТС 22600-1—2009 «Информатизация здоровья. Управление полномочиями и контроль доступа. Часть 1. Общие сведения и управление политикой»
ИСО/ТС 22600-2:2006	IDT	ГОСТ Р ИСО/ТС 22600-2—2009 «Информатизация здоровья. Управление полномочиями и контроль доступа. Часть 2. Формальные модели»
ИСО/ТС 22600-3:2009	—	*
ИСО/ТС 18308:2004	IDT	ГОСТ Р ИСО/ТС 18308—2008 «Информатизация здоровья. Требования к архитектуре электронного учета здоровья»
ИСО/ТО 22221:2006	—	*

* Соответствующий национальный стандарт отсутствует. До его утверждения рекомендуется использовать перевод на русский язык данного международного стандарта. Перевод данного международного стандарта находится в Федеральном информационном фонде технических регламентов и стандартов.

Примечание — В настоящей таблице использовано следующее условное обозначение степени соответствия стандартов:

IDT — идентичные стандарты.

Библиография

Проект SEISMED:

[1] BARBER, B., SEISMED. Data security for healthcare, IOS Press. Amsterdam; 1996. Studies in Health Technology and Informatics. ISBN: 90-5199-263-7.

[2] BARBER, B., SEISMED, Towards security in medical telematics: Legal and Technical Aspects, IOS Press. Amsterdam; 1996. Studies in Health Technology and Informatics. ISBN: 90-5199-246-7

Проект TrustHealth:

[3] BLOBEL, B. The European Trust Health Project experiences with implementing a security infrastructure, Int. J. Med. Informatics, 60, pp. 193—201, 2000

Проект HARP:

[4] BLOBEL B. Architecture of Secure Portable and Interoperable Electronic Health Records, SLOOT, P.M.A., KENNETH TAN, J.J., DONGARRA, C.J. and HOEKSTRA, A.G. (Eds.) Procs International Conference on Computational Science, April 2002, 2, pp. 982—994.

Другие публикации и дополнительные стандарты:

[5] KALRA, D. Clinical Foundations and Information Architecture for the Implementation of a Federated Health Record Service, PhD Thesis, University of London, 2003 [Доступна по адресу gost.e-ecolog.ru Kalra,%20Dipak%20(PhD%202002).pdf]

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

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

[8] ISO 17090-1, Health informatics — Public key infrastructure — Part 1: Overview of digital certificate services

[9] ISO/TS 18308, Health informatics — Requirements for an electronic health record architecture

[10] ISO/TS 21091, Health informatics — Directory services for security, communications and identification of professionals and patients

[11] ISO 21298, Health informatics — Functional and structural roles

[12] ISO 22221, Health informatics — Good principles and practices for a clinical data warehouse

[13] ISO/TS 22600-1, Health Informatics — Privilege management and access control — Part 1: Overview and policy management

[14] ISO/TS 22600-2, Health Informatics — Privilege management and access control — Part 2: Formal models

[15] ISO/TS 22600-3, Health Informatics — Privilege management and access control — Part 3: Implementations

[16] ISO 22857, Health informatics — Guidelines on data protection to facilitate trans-border flows of personal health information

[17] ISO/IEC 27002, Information technology — Security techniques — Code of practice for information security management

[18] ISO 27789, Health informatics — Audit trails for electronic health records

[19] ISO 27799, Health informatics — Security management in health using ISO/IEC 27002

[20] ENV 13608-1:2000, Health informatics — Security for healthcare communication — Part 1: Concepts and terminology

[21] ENV 13608-2:2000, Health informatics — Security for healthcare communication — Part 2: Secure data objects

[22] ENV 13608-3:2000, Health informatics — Security for healthcare communication — Part 3: Secure data channels

[23] EN 14484, Health informatics — International transfer of personal health data covered by the EU data protection directive — High level security policy

[24] EN 14485, Health informatics — Guidance for handling personal health data in international applications in the context of the EU data protection directive

[25] EN 14822-2, Health informatics — General purpose information components — Part 2: Non-clinical

[26] RFC 3881, Security Audit and Access Accountability Message — XML Data Definitions for Healthcare Applications (опубликована организацией IETF в 2004 году)

УДК 004:61:006.354 ОКС 35.240.80 П85 ОКСТУ 4002

Ключевые слова: здравоохранение, информатизация здоровья, передача электронной медицинской карты, информационная безопасность

Редактор *Н.Н. Кузьмина*
Технический редактор *В.Н. Прусакова*
Корректор *Л.Я. Митрофанова*
Компьютерная верстка *А.В. Бестужевой*

Сдано в набор 07.12.2012. Подписано в печать 30.01.2013. Формат 60×84 1/8. Гарнитура Ариал.
Усл. печ. л. 5,58. Уч.-изд. л. 4,90. Тираж 88 экз. Зак. 89.

ФГУП «СТАНДАРТИНФОРМ», 123995 Москва, Гранатный пер., 4.
gost.e-ecolog.ru gost.e-ecolog.ru
Набрано во ФГУП «СТАНДАРТИНФОРМ» на ПЭВМ.
Отпечатано в филиале ФГУП «СТАНДАРТИНФОРМ» — тип. «Московский печатник», 105062 Москва, Лялин пер., 6.

gost.e-ecolog.ru