ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р ИСО 27789— 2016

Информатизация здоровья

ЖУРНАЛЫ АУДИТА ДЛЯ ЭЛЕКТРОННЫХ МЕДИЦИНСКИХ КАРТ

ISO 27789:2013
Health informatics — Audit trails for electronic health records
(IDT)

Издание официальное

Москва
Стандартинформ
2016

gost.e-ecolog.ru

Предисловие

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

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 468 «Информатизация здоровья» при ЦНИИОИЗ Минздрава

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 5 июля 2016 г. № 806-ст

4 Настоящий стандарт идентичен международному стандарту ИСО 27789:2013 «Информатизация здоровья. Журналы аудита для электронных медицинских карт» (ISO 27789:2013 «Health informatics — Audit trails for electronic health records», IDT).

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

5 ВВЕДЕН ВПЕРВЫЕ

*Правила применения настоящего стандарта установлены в ГОСТ Р 1.0—2012 (раздел 8). Информация об изменениях к настоящему стандарту публикуется в ежегодном (по состоянию на 1 января текущего года) информационном указателе «Национальные стандарты», а официальный текст изменений и поправок — в ежемесячном информационном указателе «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ближайшем выпуске ежемесячного информационного указателя «Национальные стандарты». Соответствующая информация, уведомление и тексты размещаются также в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет (*gost.e-ecolog.ru

© Стандартинформ, 2016

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 Нормативные ссылки 1
3 Термины и определения. 2
4 Сокращения 4
5 Требования и использование данных аудита 4
5.1 Этические и формальные требования 4
5.2 Пользователи данных аудита 5
6 События срабатывания 6
6.1 Общие положения 6
6.2 Типы событий и их содержание 6
7 Содержание записи аудита 7
7.1 Общий формат записи 7
7.2 Идентификация события срабатывания 8
7.3 Идентификация пользователя 10
7.4 Идентификация точки доступа 13
7.5 Идентификация источника аудита 14
7.6 Идентификация объекта-участника 16
8 Записи аудита для отдельных событий 20
8.1 События доступа 20
8.2 События запроса 25
9 Защищенное управление данными аудита 25
9.1 Меры предосторожности 25
9.2 Обеспечение доступности системы аудита 25
9.3 Требования к хранению 25
9.4 Обеспечение конфиденциальности и целостности следов аудита 25
9.5 Доступ к данным аудита 26
Приложение А (справочное) Сценарии аудита 27
Приложение В (справочное) Сервисы журнала аудита 32
Приложение ДА (справочное) Сведения о соответствии ссылочных международных стандартов и документов национальным стандартам Российской Федерации 38
Библиография 39

Введение

0.1 Общие положения

Многие считают персональную медицинскую информацию одним из самых конфиденциальных типов личной информации, и защита ее конфиденциальности необходима, если предполагается обеспечение неприкосновенности личности субъектов получения медицинской помощи. Для защиты согласованности медицинской информации также важно, чтобы весь ее жизненный цикл был полностью проверяемым. Медицинские карты должны создаваться, обрабатываться, управляться методами, гарантирующими целостность и конфиденциальность их содержания, и предоставлять субъектам получения медицинской помощи правомочный контроль того, как эти карты создаются, используются и обслуживаются.

Для обеспечения доверия к медицинским картам требуются элементы физической и технической защиты наряду с элементами целостности данных. Одними из самых важных требований к защите персональной медицинской информации и целостности записей являются требования, связанные с аудитом и ведением журнала. Эти требования помогают обеспечить учетность для субъектов получения медицинской помощи, которые доверяют свою информацию системам электронных медицинских карт (EHR). Они также помогают защитить целостность записей, так как серьезно стимулируют пользователей таких систем соответствовать организационной политике по использованию таких систем.

Эффективный аудит и ведение журнала могут помочь выявить ненадлежащее использование систем EHR или данных EHR, а также могут защитить организации и субъекты получения медицинской помощи от пользователей, злоупотребляющих их полномочиями доступа. Для обеспечения эффективности аудита необходимо, чтобы аудиторский след содержал объем информации, достаточный для решения широкого спектра задач (см. приложение А).

Журналы аудита являются дополнением к средствам управления доступом. Журналы аудита предоставляют средства для оценки соответствия с политикой доступа организации и вносят свой вклад в улучшение и совершенствование самой политики. Но ввиду того, что такая политика должна предугадывать возможность непредвиденных или аварийных ситуаций, анализ аудита становится основным средством обеспечения управления доступом для таких ситуаций.

Область применения настоящего стандарта строго ограничена ведением журнала событий. Предполагается, что изменения значений данных в полях EHR должны записываться в саму систему базы данных EHR, а не в журнал аудита. Предполагается, что сама система EHR содержит и предыдущие, и обновленные данные каждого поля. Это соответствует современной архитектуре базы данных «по состоянию на определенный момент времени». Сам журнал аудита не должен содержать персональную медицинскую информацию, кроме идентификаторов и ссылок на запись.

Электронные медицинские карты отдельного человека могут располагаться в разных информационных системах в пределах одной организации или в разных организациях, или даже в разных юрисдикциях. Для отслеживания всех действий, включающих записи по различным объектам оказания медицинской помощи, необходима общая структура. Настоящий стандарт предоставляет такую структуру. Для поддержки аудиторских следов в различных доменах необходимо включать ссылки в данной структуре на политику, которая определяет требования в пределах домена, такие как правила контроля доступа и период хранения. На политику домена можно делать косвенные ссылки посредством идентификации источника журнала аудита.

0.2 Преимущества использования настоящего стандарта

Стандартизация следов аудита по доступу к электронным медицинским картам преследует две цели:

- обеспечение того, что объем информации, отображенной в журнале аудита, является достаточным для четкого воссоздания подробной хронологии событий, сформировавших содержание электронной медицинской карты, и
- обеспечение того, что аудиторский след действий, связанных с картой субъекта получения медицинской помощи, может достоверно отслеживаться даже с учетом организационных структур в разных предметных областях.

Настоящий стандарт предназначен для лиц, ответственных за надзор за защитой или конфиденциальностью медицинской информации, для медицинских организаций и других хранителей медицин-

ской информации, обращающихся за руководящими указаниями по аудиторским следам, а также их советников по защите, консультантов, аудиторов, продавцов и третьих лиц, оказывающих услуги.

0.3 Сравнение со стандартами, связанными с аудиторскими следами электронных медицинских карт

Настоящий стандарт соответствует требованиям ИСО 27799:2008, в той части, в которой они связаны с выполнением аудита и аудиторскими следами.

Некоторые читатели могут быть знакомы с Запросом Комментариев (RFC) Рабочей группы инженеров Интернет (IETF RFC 3881 [13]). (Читатели, еще не знакомые с IETF RFC 3881, не должны ссылаться на данный документ, так как осведомленность в этом вопросе не требуется для понимания настоящего стандарта.) Информационный RFC 3881 от 2004-09, не указанный на сегодняшний день среди действующих запросов в базе данных IETF, был ранней и полезной попыткой определения содержания журналов аудита для здравоохранения. Настоящий стандарт по мере возможности основывается и согласуется с работой, начатой в RFC 3881 по доступу к EHR.

0.4 Примечание по терминологии

В разделе 3 определено несколько близко связанных терминов. Журнал аудита — это хронологическая последовательность записей аудита; каждая запись аудита содержит доказательство того, что она имеет прямое отношение к процессу или системной функции и возникает в результате их выполнения. Так как системы EHR могут быть сложными, может существовать несколько журналов аудита, содержащих информацию о событиях системы, которые изменили EHR субъекта получения медицинской помощи. Хотя термины «аудиторский след» и «журнал аудита» часто используются как взаимозаменяемые понятия, в настоящем стандарте термин «аудиторский след» относится к совокупности всех записей аудита из одного или нескольких журналов аудита, относящихся к определенному субъекту получения медицинской помощи, к определенной электронной медицинской карте или определенному пользователю. Система аудита предоставляет все функции обработки информации, необходимые для обслуживания одного или нескольких журналов аудита.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ИНФОРМАТИЗАЦИЯ ЗДОРОВЬЯ

Журналы аудита для электронных медицинских карт

Health informatics. Audit trails for electronic health records

Дата введения — 2017—07—01

1 Область применения

Настоящий стандарт определяет общую структуру аудиторских следов для электронных медицинских карт (EHR), в терминах контрольных событий аудита и данных аудита, для поддержки контролируемости всего набора персональной медицинской информации в разных информационных системах и предметных областях.

Настоящий стандарт применим к системам обработки персональной медицинской информации, которые в соответствии с ИСО 27799 создают защищенную запись аудита каждый раз, когда пользователь получает доступ, создает, обновляет или архивирует персональную медицинскую информацию в системе.

Примечание — Такие записи аудита, как минимум, однозначно идентифицируют пользователя, однозначно идентифицируют субъект получения медицинской помощи, идентифицируют функцию, выполняемую пользователем (создание, доступ, обновление записи и т. д.), и записывают дату и время, в которое была выполнена эта функция.

Настоящий стандарт охватывает только действия, выполняемые с помощью EHR, которые подчиняются политике обеспечения доступа к предметной области, для которой электронная медицинская карта была выпущена. Настоящий стандарт не относится к какой-либо персональной медицинской информации из электронной медицинской карты, кроме идентификаторов, запись аудита содержит только ссылки на разделы EHR, как указано в применяемой политике доступа.

В настоящем стандарте не рассматриваются характеристики и использование журналов аудита в целях управления системой и обеспечения защиты системы, таких как определение проблем производительности, недостатков программы или поддержка при восстановлении данных, которые рассматриваются в общих стандартах по компьютерной безопасности, таких как ИСО/МЭК 15408-2 [9].

В приложении А представлены примеры сценариев аудита. Приложение В содержит обзор сервисов журнала аудита.

2 Нормативные ссылки

Следующие нормативные документы являются обязательными для применения настоящего документа. Для датированных ссылок применяется только цитированное издание. Для недатированных ссылок применяется последнее издание ссылочного документа (включая все поправки).

ИСО 8601:2004 Элементы данных и форматы для обмена информацией. Обмен информацией. Представление дат и времени (ISO 8601:2004, Data elements and interchange formats — Information interchange — Representation of dates and times)

ИСО 27799:2008 Информатизация здоровья. Менеджмент безопасности информации по стандарту ИСО/МЭК 27002 (ISO 27799:2008, Health informatics — Information security management in health using ISO/МЭК 27002)

Издание официальное

3 Термины и определения

В настоящем стандарте применены следующие термины и определения.

3.1

контроль доступа (access control): Обеспечение того, чтобы доступ к активам был санкционирован и ограничен в соответствии с требованиями коммерческой тайны и безопасности.

[ИСО/МЭК 27000:2012, определение 2.1]

3.2 **политика доступа** (access policy): Определение обязанностей по санкционированию доступа к ресурсу.

3.3

учетность (accountability): Принцип, заключающийся в том, что отдельные лица, организации и сообщества несут ответственность за свои действия, и от них могут потребовать объяснить их действия.

[ИСО 15489-1:2001, определение 3.2]

3.4 **аудит** (audit): Систематическая и независимая проверка доступа, добавлений или изменений информации в электронных медицинских картах для определения того, были ли такие действия выполнены, а данные собраны, использованы, сохранены или раскрыты в соответствии с установленными принципами работы организации, политикой, надлежащей клинической практикой и применимыми нормативными требованиями.

3.5 **архив аудита** (audit archive): Архивная коллекция одного или нескольких журналов аудита.

3.6 **данные аудита** (audit data): Данные, полученные из одного или нескольких журналов аудита.

3.7 **журнал аудита** (audit log): Хронологическая последовательность записей аудита, каждая из которых содержит данные об определенном событии.

3.8 **запись аудита** (audit record): Запись одного определенного события в жизненном цикле электронной медицинской карты.

3.9 **система аудита** (audit system): Система обработки информации, которая поддерживает работу одного или нескольких журналов аудита.

3.10 **аудиторский след** (audit trail): Коллекция записей аудита от одного или нескольких журналов аудита, связанных с определенным субъектом получения медицинской помощи или определенной электронной медицинской картой.

3.11 **аутентификация** (authentication): Обеспечение гарантии того, что заявленные характеристики объекта являются правильными.

3.12 **авторизация** (authorization): Предоставление полномочий, включая полномочия по данным и функциям доступа.

Примечание — Основано на ИСО 7498-2. Предоставление прав, включая предоставление доступа на основании прав доступа.

3.13 **орган** (authority): Субъект, ответственный за выдачу сертификатов.

3.14

доступность (availability): Свойство быть доступным и готовым к использованию по запросу авторизованного субъекта.

[ИСО/МЭК 27000:2012, определение 2.10]

3.15

конфиденциальность (confidentiality): Свойство информации быть недоступной или закрытой для неавторизованных лиц, сущностей или процессов.

[ИСО/МЭК 27000:2012, определение 2.13]

3.16

всемирное скоординированное время (Coordinated Universal Time; UTC): Шкала времени, составляющая основу для скоординированной передачи по радио стандартных частот и сигналов времени; она точно соответствует по частоте Международному Атомному Времени, но отличается от него целым числом секунд.

[МЭК 60050-713:1998]

3.17

целостность данных (data integrity): Свойство, заключающееся в том, что данные не были изменены или уничтожены несанкционированным способом.

[ИСО 7498-2:1989, определение 3.3.21]

3.18

электронная медицинская карта (Electronic health record; EHR): Всесторонний структурированный комплекс клинических, демографических данных, данных об окружающей среде, социальных и финансовых данных в электронной форме, документирующий оказание медицинских услуг отдельному человеку.

[ASTM E 1769:1995]

3.19 **сегмент EHR** (EHR segment): Часть EHR, которая составляет определенный источник для политики доступа.

3.20

идентификация (identification): Проведение проверок, которые позволяют системе обработки данных распознать сущности.

[ИСО/МЭК 2382-8:1998, определение 08.04.12 [как аутентификация личности (identity authentication), проверка личности (identity validation)]

3.21 **идентификатор** (identifier): Информация, используемая для утверждения личности перед возможным ее подтверждением соответствующим аутентификатором.

3.22

защищенность информации (information security): Сохранение конфиденциальности, целостности и доступности информации.

[ИСО/МЭК 27000:2012, определение 2.30]

3.23

целостность (integrity): Свойство сохранения правильности и полноты активов.

[ИСО/МЭК 27000:2012, определение 2.36]

3.24 **идентификатор объекта** (object identifier; OID): Глобальный уникальный идентификатор для информационного объекта.

Примечание — Идентификаторы объекта, использованные в настоящем стандарте, относятся к кодовым системам. Эти кодовые системы могут быть определены в стандарте или локально определены при внедрении. Идентификатор объекта устанавливается с использованием языка ASN.1 для описания абстрактного синтаксиса (ASN.1), определенного в ИСО/МЭК 8824-1 и ИСО/МЭК 8824-2.

3.25

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

[ИСО/ТС 22600]

3.26 **полномочие** (privilege): Возможность, закрепленная органом за субъектом.

3.27

управление записями (records management): Область управления, которая отвечает за эффективный и систематический контроль над созданием, выдачей, сохранением, использованием и изъятием из обращения записей, включая сбор и поддержание доказательств и информации о деловой деятельности и транзакциях в виде записей.

[ИСО 15489-1, определение 3.16]

3.28 **роль** (role): Комплекс умений и/или действий, связанных с задачей.

3.29 **чувствительность** (sensitivity): Возможность или кажущаяся возможность по причинению вреда субъекту данных или его возможность стать объектом злоупотребления или неправильного использования.

3.30 **политика защищенности** (security policy): План или образ действий, принятый для предоставления компьютерной защищенности.

3.31

субъект медицинской помощи (subject of care): Лицо, которому запланирована медицинская помощь, получающее или получившее медицинскую помощь.

[ИСО 18308:2011, определение 3.47]

3.32 **пользователь** (user): Человек, устройство или программа, использующая систему EHR для обработки данных или обмена медицинской информацией.

4 Сокращения

EHR — Электронная медицинская карта (Electronic Health Record);

HL7 — Международная организация — разработчик стандартов по информатизации здоровья (Health Level Seven International);

OID — Идентификатор объекта (Object Identifier);

UTC — Всемирное Скоординированное Время (Coordinated Universal Time).

5 Требования и использование данных аудита

5.1 Этические и формальные требования

5.1.1 Общие положения

У поставщиков медицинской помощи есть профессиональные этические обязанности. К ним относятся защита конфиденциальности объектов получения медицинской помощи и документирование результатов и действий по уходу. Ограничение доступа к медицинским картам и обеспечение их надлежащего использования являются важными требованиями здравоохранения, и во многих юрисдикциях эти требования прописаны в законе.

Защищенные следы аудита по доступу к электронным медицинским картам могут поддерживать соответствие с профессиональной этикой, организационной политикой и законодательством, но их самих недостаточно для того, чтобы оценить полноту электронной медицинской карты.

5.1.2 Политика доступа

Организация, ответственная за поддержание работоспособности журнала аудита, должна определить политику доступа, регламентирующую все зарегистрированные случаи доступа.

Политика доступа должна соответствовать ИСО 27799:2008, 7.8.1.2, Политика контроля доступа.

Примечания

1 Считается, что политика доступа должна определять структуру сегмента EHR.

2 В записи аудита политика доступа идентифицируется источником журнала аудита.

Руководство по определению и применению политик доступа можно найти в ИСО/ТС 22600 [6]. Поле «Participant object Permission Policy Set» определено в п. 7.6.6 для поддержки ссылок на действующие политики в записи аудита.

5.1.3 Однозначная идентификация пользователей информационной системы

Аудиторские следы должны предоставлять достаточный объем данных для того, чтобы однозначно определить всех авторизованных пользователей системы медицинской информации. Пользователями информационной системы могут быть люди, а также другие сущности.

Аудиторские следы должны предоставлять достаточный объем данных для того, чтобы определить, какие авторизованные пользователи и внешние системы получили доступ и которым из них были отправлены данные медицинских карт из системы.

5.1.4 Роли пользователей

Аудиторский след должен показывать роль пользователя при осуществления записанного действия по отношению к персональной медицинской информации.

Информационные системы, занимающиеся обработкой персональной медицинской информации, должны поддерживать ролевой доступ, способный связывать каждого пользователя с одной или не-

сколькими ролями, а каждую роль к одной или нескольким системным функциям, как рекомендовано в ИСО 27799:2008, 7.8.2.2, Управление полномочиями.

Функциональные и структурные роли задокументированы в ИСО/ТС 21298 [4]. Дополнительные руководства по управлению полномочиями в здравоохранении представлены в ИСО/ТС 22600 [6]

5.1.5 Защищенные записи аудита

Защищенные записи аудита должны создаваться каждый раз, когда к персональной медицинской информации осуществляется доступ или когда она создается, обновляется или архивируется в соответствии с ИСО 27799:2008, 7.7.10.2, Ведение журнала аудита. Записи аудита должны поддерживаться управлением защищенными записями.

5.2 Пользователи данных аудита

5.2.1 Управление и контроль

Аудиторские следы должны предоставлять данные, позволяющие ответственным органам оценивать соответствие с политикой организации и оценивать ее эффективность.

Под этим подразумевается:

- обнаружение несанкционированного доступа к медицинским картам,
- оценка экстренного доступа,
- обнаружение злоупотребления полномочиями

и поддерживается:

- документально оформленный доступ к предметным областям и
- оценка политик доступа.

Примечание — Полная оценка соответствия политике организации может потребовать предоставление дополнительных данных, которые не содержатся в записи аудита, таких как информация о пользователе, таблица полномочий или записи по физическому доступу к защищенным помещениям. См. в приложении В информацию о сервисах журналов аудита.

Аудиторские следы должны предоставлять достаточный объем данных для определения всех случаев доступа к картам субъектов получения медицинской помощи конкретным пользователем в пределах заданного промежутка времени.

Аудиторские следы должны предоставлять достаточный объем данных для определения всех случаев доступа к картам субъектов получения медицинской помощи, о которых известно, что для них повышен риск нарушения конфиденциальности.

5.2.2 Осуществление прав субъектов получения медицинской помощи

Аудиторские следы должны предоставлять достаточный объем данных для того, чтобы позволить субъектам получения медицинской помощи:

- определять, какие авторизованные пользователи имели доступ к его/ее медицинской карте и когда это происходило,
- оценивать учетность для содержания карты,
- определять соответствие с директивами согласия субъекта получения медицинской помощи на доступ или разглашение данных субъекта получения медицинской помощи и
- определять экстренный доступ (при наличии такового), предоставляемый пользователю, к карте субъекта получения медицинской помощи, включая идентификацию пользователя, время доступа и место доступа.

5.2.3 Этические и юридические доказательства деятельности поставщика медицинской помощи

Аудиторские следы должны предоставлять данные для обеспечения поставщиков медицинской помощи документальными доказательствами того, как демонстрировалась информация и какие действия были выполнены (создание, просмотр, чтение, исправление, обновление, выделение, выведение, архивирование и т. д.), с информацией, когда и кем они были предприняты.

Сохранение записей аудита должно быть согласовано с юридическими условиями учетности в пределах юрисдикции.

См. Управление документами и подтверждение доказательствами (RM-ES) для EHR в HL7.

6 События срабатывания

6.1 Общие положения

События аудита (события срабатывания), которые приводят к тому, что система аудита создает записи аудита, определены в соответствии с масштабом, целью и содержанием политик конфиденциальности и защиты каждой системы медицинской информации. Область применения настоящего стандарта ограничена доступом к персональной медицинской информации, поэтому указаны только события срабатывания, связанные с доступом.

Для создания записей аудита, соответствующих требованиям, представленным в 5, т. е. «когда», «кто», «чей», следующие два события являются обязательными:

a) события доступа к персональной медицинской информации;

b) события запроса персональной медицинской информации.

Примеры событий, не входящих в область применения настоящего стандарта:

- события запуска и остановки программы приложения;
- события аутентификации, включающие аутентификацию пользователей;
- события ввода и вывода из/во внешнюю среду;
- события доступа к информации, отличной от персональной медицинской информации;
- события сигналов тревоги защиты, связанные с программой приложения;
- события доступа к журналу аудита, сохраненному в программе приложения;
- события, созданные операционной системой, промежуточным программным обеспечением и т. д.;
- события доступа, созданные посредством использования системных утилит;
- события физического подключения/отключения оборудования от сети;
- события запуска/остановки систем защиты, таких как системы антивирусной защиты;
- события обновления программного обеспечения, включая модификацию программного обеспечения или патчи.

6.2 Типы событий и их содержание

6.2.1 События доступа к персональной медицинской информации

В настоящем стандарте доступ к персональной медицинской информации рассматривается как событие аудита. Здесь «Доступ» означает создание, чтение, обновление, удаление данных. Содержание журнала аудита предоставляет информацию о данных доступа («когда», «кто», «доступ к чьей информации»), подлежащих защите. См. таблицу 1.

Таблица 1 — События доступа

События	Содержание
События доступа к персональной медицинской информации	Когда Кто Доступ к чьей информации

6.2.2 События запроса персональной медицинской информации

Запрос в базу данных EHR с целью получения информации рассматривается как событие, подвергаемое аудиту. Событие запроса — это сам запрос, ссылка на персональную медицинскую информацию, возникающая в результате запроса, считается событием доступа. Содержание записи аудита предоставляет информацию о запросе («когда», «кто», «какие условия запроса»). См. таблицу 2.

Таблица 2 — События запроса

События	Содержание
События запроса персональной медицинской информации	Когда Кто Какие условия запроса

7 Содержание записи аудита

7.1 Общий формат записи

Таблица 3 описывает общий формат записей аудита. О содержании записи по каждому событию см. 8. Формат записи определяется в соответствии с RFC 3881 [13] и DICOM [11] с добавлением дополнительных полей PurposeOfUse (ЦельИспользования) и «ParticipantObjectPolicySet» (КомплексПолитикОбъектовУчастников).

Таблица 3 — Общий формат записей аудита

Тип	Имя поля	Важность	Описание	Дополнительная информация
Связанное с событием (1)	EventID	M	Идентификатор события, проверяемого аудитом	См. п. 7.2
	EventActionCode	M	Тип действия, выполненного во время события, проверяемого аудитом	
	EventDateTime	M	Дата/время наступления события, проверяемого аудитом	
	EventOutcomeIndicator	U	Успех или неудача события	
	EventTypeCode	U	Категория события	
Связанное с пользователем (1..2)	UserID	M	Идентификатор пользователя или процесса	См. п. 7.3
	AlternateUserID	U	Альтернативный идентификатор пользователя или процесса	
	UserName	U	Имя пользователя или процесса	
	UserIsRequestor	U	Индикатор того, что пользователь является или не является инициатором запроса	
	RoleIDCode	U	Спецификация роли, которую играет пользователь в исполнении события	
	PurposeOfUse	U	Код цели использования данных, к которым осуществлен доступ	
	NetworkAccessPoint TypeCode	U	Тип точки доступа к сети	См. п. 7.4
	NetworkAccessPointID	U	Идентификатор точки доступа к сети	
Связанное с системой аудита (1)	AuditEnterpriseSiteID	U	Идентификатор участка предприятия аудита	См. п. 7.5
	AuditSourceID	M	Уникальный идентификатор источника аудита	
	AuditSourceTypeCode	U	Код типа источника аудита	
Связанное с объектом-участником (0..N)	ParticipantObject TypeCode	M	Код типа объекта-участника	См. п. 7.6
	ParticipantObject TypeCodeRole	M	Тип кода объекта роли	
	ParticipantObjectData LifeCycle	U	Идентификатор этапа жизненного цикла данных для объекта-участника	
	ParticipantObjectID TypeCode	M	Код типа идентификатора объекта-участника	
	ParticipantObject PolicySet	U	Комплекс политик доступа для идентификатора объекта-участника	

Окончание таблицы 3

Тип	Имя поля	Важность	Описание	Дополнительная информация
Связанное с объектом-участником (0..N)	ParticipantObject Sensitivity	U	Чувствительность, определенная политикой для Идентификатора объекта-участника	См. п. 7.6
	ParticipantObjectID	M	Определяет частный случай объекта-участника	
	ParticipantObjectName	U	Имя объекта-участника, например имя человека	
	ParticipantObjectQuery	M/U	Содержание запроса для объекта-участника	
	ParticipantObjectDetail	U	Информация по объекту-участнику	
Множественность		Степень важности		
(1)		M	Обязательное	
(0..1)	существует 0 или 1	MC	Условно-обязательное	
(1..2)	существует 1 или 2	U	Необязательное	
(0..N)	существует от 0 до N	M/U	Обязательное или необязательное в зависимости от события	

7.2 Идентификация события срабатывания

7.2.1 Идентификатор события (Event ID)

Описание. Уникальный идентификатор для определенного события, проверяемого аудитом, например пункт меню, программа, правило, политика, код функции, имя приложения или URL. Он определяет выполняемую функцию.

Степень важности. Обязательное.

Формат/Значения. Закодированное значение, либо определенное разработчиками системы, либо упоминаемое в словаре стандарта. Атрибут «code» («атрибут») должен быть недвусмысленным и уникальным, по крайней мере, в пределах ID (Идентификатора) источника аудита (см. п. 7.5). Примерами ID событий являются имя программы, имя метода или имя функции.

Примечание — Кодирование выстраивается по образцу IHEITITF-1 и TF-1 [12] и ИСО 12052 [1], дополнение 95 к DICOM [11].

Схема XML в RFC 3881 определяет дополнительные атрибуты для определенных реализацией закодированных значений или ссылок на стандарты (см. таблицу 4).

Таблица 4 — Ссылочные атрибуты ID события

Атрибут	Значение
CodeSystem (СистемаКода)	Ссылка на OID
CodeSystemname (ИмяСистемыКодирования)	Имя системы кодирования; настоятельно рекомендуется учитывать для локально определенных кодовых наборов
CodeValue (ЗначениеКода)	Определенный код в пределах системы кодирования
DisplayName (ОтображаемоеИмя)	Значение, которое должно быть использовано при демонстрации и в отчетах
OriginalText (ИсходныйТекст)	Входное значение, которое было переведено в код

Для выполнения требования однозначной идентификации события множественные значения можно не определять.

Логическое обоснование. Данное поле идентифицирует функцию, проверяемую аудитом. В случае записей аудита кода действия события «Execute» («Выполнить») данное поле идентифицирует выполненную функцию приложения.

По крайней мере, один из атрибутов, CodeSystem (OID) или CodeSystemName, является обязательным.

7.2.2 Код действия события (EventID)

Описание. Идентификатор типа действия, выполненного в событии аудита.

Степень важности. Обязательное.

Формат/Значения. Перечислены в таблице 5.

Таблица 5 — Коды действия события

Значение	Значение	Примеры
C	Создать	Создать новый объект базы данных, например размещение заказа
R	Прочитать/ Показать/ Распечатать/ Запрос	Отобразить или распечатать данные, например диагноз
U	Обновить	Обновить данные, например внесение изменений в персональную медицинскую информацию
D	Удалить	Сделать объекты недоступными
E	Выполнить	Выполнить функцию системы или приложения, например поиск, извлечение или использование метода объекта

Логическое обоснование. Данное поле в широком смысле обозначает, какой вид действия был выполнен над объектом-участником.

Примечания

1 Действия, не перечисленные выше, рассматриваются как Выполнить определенную функцию или метод интерфейса объекта или рассматриваются как два или более отдельных событий. Действие приложения, такое как авторизация или использование цифровой подписи, является функцией Выполнить, а ID события ее идентифицирует.

2 Для некоторых приложений, таких как рентгеновская визуализация, действие Запрос может определить только наличие данных, но не предоставить доступ к самим данным. Проведение аудита не всегда требует такого тонкого разграничения.

3 Комбинированные действия, такие как «Переместить», «Заархивировать» или «Скопировать», будут проверяться аудитом посредством создания данных аудита для каждой операции — чтения, создания, удаления — или операций Выполнения функции или метода.

7.2.3 Дата и время события (Event date and time)

Описание. Определение даты/времени, являющееся однозначным по отношению к местным часовым поясам.

Степень важности. Обязательное.

Формат/Значения. Представление даты/времени, являющееся однозначным при передаче всемирного скоординированного времени (UTC). Время должно быть в формате UTC, как в ИСО 8601:2004, и иметь расхождение с UTC не более 250 мс.

Логическое обоснование. Данное поле привязывает событие к определенным дате и времени. Аудиты защиты обычно требуют соответствующую временную ось для устранения проблем, связанных с часовыми поясами, возникающих из-за географического распределения.

Примечание — В распределенной системе хорошей тактикой внедрения является использование своего рода общей временной оси, например, NTP сервера [RFC1305].

7.2.4 Индикатор результата события (Event outcome indicator)

Описание. Обозначает, было ли событие успешным или неуспешным.

Степень важности. Необязательное.

Формат/Значения. Закодированное значение. Код ноль (0) обозначает успех события. Значения неуспеха события не имеют значимости в пределах области применения настоящего стандарта.

Логическое обоснование. Данное поле предназначено для сохранения совместимости со следами аудита согласно IETFRFC 3881 [13].

7.2.5 Код типа события (Event type code)

Описание. Идентификатор категории события.

Степень важности. Необязательное.

Формат/Значения. Перечисление закодированных значений, либо определенные разработчиками системы, либо упоминаемое в словаре стандарта. Схема XML в RFC 3881 определяет дополнительные атрибуты для определенных реализацией закодированных значений или значений, упоминаемых в стандарте, показанных в таблице 6.

Таблица 6 — Ссылочные атрибуты кода типа события

Атрибут	Значение
CodeSystem	Ссылка на OID
CodeSystemname	Имя системы кодирования; настоятельно рекомендуется учитывать для локально определенных кодовых наборов
DisplayName	Значение, которое должно быть использовано при демонстрации и в отчетах
OriginalText	Входное значение, которое было переведено в код

События могут быть классифицированы более чем одним способом, поэтому могут быть обозначены различные значения.

Логическое обоснование. Данное поле позволяет делать запросы записей аудита посредством определенных реализацией категорий событий.

7.3 Идентификация пользователя

7.3.1 Идентификатор пользователя (User ID)

Описание. Уникальный идентификатор для пользователя, принимающего активное участие в событии.

Степень важности. Обязательное.

Формат/Значения. Текстовая строка идентификатора пользователя из системы аутентификации. Уникальное значение в пределах Идентификатора Источника события (см. п. 7.4).

Логическое обоснование. Данное поле привязывает событие аудита к определенному пользователю. В данном контексте пользователь может быть человеком, группой, командой, сервером, процессом или потоком задач.

Примечания

1 Для межсистемных аудитов, особенно с долгим хранением, данный идентификатор пользователя предназначен для постоянной привязки события аудита к определенному пользователю посредством уникального ключа, который сохраняет свою уникальность в течение всего срока действия архивирования аудиторских следов.

2 Для узловой аутентификации, где идентифицируется только оборудование или процессы системы, а не пользователь-человек, Идентификатор пользователя считается именем узла.

3 Если аудиторский след должен быть использован для клинического аудита или для того, чтобы при необходимости предоставить доказательства ненадлежащего использования, аудиторский след должен однозначно ассоциировать уникальный идентификатор с реальным пользователем.

7.3.2 Альтернативный идентификатор пользователя (Alternative user ID)

Описание. Альтернативный уникальный идентификатор для пользователя.

Степень важности. Необязательное.

Формат/Значения. Текстовая строка идентификатора пользователя из системы аутентификации. Данный идентификатор, при его наличии, будет известен общей системе аутентификации.

Логическое обоснование. В некоторых ситуациях пользователь может аутентифицироваться одним средством идентификации, но для того, чтобы войти в определенную систему приложения, он может использовать равнозначные средства идентификации. В таком случае альтернативный идентификатор будет являться оригинальным средством идентификации, используемым для аутентификации, а Идентификатор пользователя является известным приложению и используемым им.

7.3.3 Имя пользователя (User name)

Описание. Значимое для человека имя пользователя.

Степень важности. Необязательное.

Формат/Значения. Текстовая строка.

Логическое обоснование. Идентификатор пользователя и Альтернативный идентификатор пользователя могут быть внутренними или же скрытыми значениями. Данное поле помогает аудитору при идентификации реального пользователя.

7.3.4 Пользователь — инициатор запроса (User is requestor)

Описание. Индикатор того, что пользователь является или не является запрашивающим или инициатором для события, проходящего проверку аудитом.

Степень важности. Необязательное.

Формат/Значения. Булевское значение, стандартное/принятое значение — «true» («истина»).

Логическое обоснование: Данное значение используется для разграничения запрашивающих пользователей и пользователей-получателей. Например, отчет может быть найден пользователем (запрашивающим). Или пользователь (запрашивающий) может запустить отправку вывода отчета другому пользователю (который является получателем отчета, а не запрашивающим).

7.3.5 Идентификационный код роли (Role ID code)

Описание. Спецификация роли, которую играет пользователь в исполнении события, как прописано в защите ролевого доступа. Такие системы ролевого доступа привязывают каждого пользователя к одной или нескольким ролям, а каждую роль — к одной или нескольким системным функциям.

Степень важности. Необязательное, с множеством значений.

Формат/Значения. Закодированное значение с атрибутом «code», которому присвоено значение кода роли или текст от системы авторизации. Может быть указано несколько значений, так как может использоваться несколько систем ролевого доступа и/или классификаций. Обратите внимание, что и в ИСО 27799:2008, п. 7.8.2.2 (Управление полномочиями), и в ИСО/ТС 22600 [6] указывается, что пользователь системы медицинской информации, содержащей персональную медицинскую информацию, имеет доступ к сервисам в единственной роли (т. е. пользователям, зарегистрированным с несколькими ролями, приписывается единственная роль во время каждого сеанса доступа к системе медицинской информации).

Рекомендуется использовать систему кодирования, совместимую с функциональными ролями, определенными в ИСО/ТС 21298 [4] и перечисленными в таблице 7.

На идентификацию словаря для данного списка закодированных значений может ссылаться следующий OID, обозначенный с использованием Языка ASN.1 для описания абстрактного синтаксиса (ASN.1), определенного в ИСО/МЭК 8824-1 [7] и ИСО/МЭК 8824-2 [8].

Идентификация словаря. ИСО (1) стандарт (0) функциональные и структурные роли (21298) словарь функциональных ролей (4).

Таблица 7 — Идентификационные коды функциональных ролей

role_identifier	role_name	Описание
01	Субъект получения медицинской помощи	Основной субъект данных электронной медицинской карты
02	Агент субъекта получения медицинской помощи	Например, родитель, опекун, лицо, осуществляющее уход, или другой законный представитель
03	Персональный работник здравоохранения	Работник или работники здравоохранения, находящиеся в тесной связи с пациентом, часто семейный врач пациента
04	Уполномоченный работник здравоохранения	Назначается субъектом получения медицинской помощи ИЛИ назначается медицинским учреждением (при назначении руководством, практикой и т. д., например, функция аварийного обхода)
05	Работник здравоохранения	Сторона, вовлеченная в предоставление прямой медицинской помощи пациенту
06	Работник лечебно-оздоровительных учреждений	Сторона, косвенно вовлеченная в уход за пациентом, обучение, исследование и т. д.
07	Администратор	Любые другие стороны, поддерживающие оказание услуг пациенту

Данное поле идентифицирует список функциональных ролей высшего уровня для обеспечения возможности интероперабельного обмена между юрисдикциями и предметными областями. Оно может применяться для управления созданием, доступом, обработкой и передачей медицинской информации. Более детализированные функциональные роли могут быть присвоены в пределах предметной области или юрисдикции или могут быть оговорены для обмена информацией между такими предметными областями или юрисдикциями.

Коды могут быть определены реализацией или упоминаться в перечислении в словаре стандарта. Схема XML в RFC 3881 определяет дополнительные атрибуты для определенных реализацией закодированных кодов или кодов, упоминаемых в стандарте, как показано в таблице 8.

Таблица 8 — Ссылочные атрибуты кода идентификатора роли

Атрибут	Значение
CodeSystem	Ссылка на OID
CodeSystemname	Имя системы кодирования; настоятельно рекомендуется учитывать для локально определенных кодовых наборов
DisplayName	Значение, которое должно быть использовано при демонстрации и в отчетах
OriginalText	Входное значение, которое было переведено в код

Логическое обоснование. Данное поле привязывает событие аудита к роли пользователя. Данная роль является ключевым элементом в политиках для контроля доступа к персональной медицинской информации.

Дополнительную информацию можно найти в ИСО/ТС 22600 [6] и ИСО/ТС 21298 [4].

7.3.6 Цель использования (Purpose of use)

Описание. Обозначает цель, с которой будет использована персональная медицинская информация, к которой получен доступ.

Степень важности. Необязательное.

Формат/Значения. Перечисление закодированных значений либо зависимых от реализации, либо упоминаемых в словаре стандарта.

Рекомендуется использовать систему кодирования, совместимую со схемой классификации целей для обработки персональной медицинской информации, определенных в ИСО/ТС14265 [2] и перечисленных в таблице 9.

На идентификацию словаря для данного списка закодированных значений может ссылаться следующий OID, обозначенный с использованием языка ASN.1 для описания абстрактного синтаксиса (ASN.1), определенного в ИСО/МЭК 8824-1 [7] и ИСО/МЭК 8824-2 [8].

Идентификация словаря. ИСО (1) стандарт (0) Классификация целей для обработки персональной медицинской информации (14265) Терминология для классификации целей для обработки персональной медицинской информации (1).

Таблица 9 — Классификация целей

Код	Термин классификации	Описание (информативное)
1	Оказание клинической помощи отдельному субъекту получения медицинской помощи	Для информирования лиц или процессов, ответственных за предоставление медицинских услуг субъекту получения медицинской помощи
2	Оказание неотложной помощи отдельному субъекту получения медицинской помощи	Для информирования лиц, которые должны незамедлительно предоставить медицинские услуги субъекту получения медицинской помощи, возможно, требуя политик соглашения и замещения, отличных от относящихся к цели 1, указанной выше
3	Поддержка действий по уходу в пределах организации поставщика услуг для отдельного субъекта получения медицинской помощи	Для информирования лиц или процессов, позволяющих другим предоставлять медицинские услуги субъекту получения медицинской помощи, посредством управления действиями и/или средствами

Окончание таблицы 9

Код	Термин классификации	Описание (информативное)
4	Обеспечение возможности оплаты предоставления помощи отдельному субъекту получения медицинской помощи	Для информирования лиц или процессов, обеспечивающих доступность фондов и/или разрешений со стороны плательщика для предоставления медицинских услуг субъекту получения медицинской помощи
5	Управление и обеспечение качества медицинского обслуживания	Для информирования лиц или процессов, ответственных за определение доступности, качества, безопасности, справедливости и рентабельности медицинских услуг
6	Образование	Для поддержки образовательного и профессионального развития работника здравоохранения
7	Наблюдение за здоровьем населения	Для информирования лиц или процессов, курирующих вопросы мониторинга населения и групп населения на предмет крупных событий в сфере здравоохранения и последующего вмешательства с целью предоставления услуг здравоохранения или профилактических услуг для соответствующих лиц
8	Чрезвычайные ситуации, являющиеся угрозой для общественной безопасности	Для информирования лиц, ответственных за защиту общества, в ситуациях, когда считается, что имеет место значительный риск для членов общества, возможно, требуя политик соглашения и замещения, отличных от относящихся к Цели 7, указанной выше
9	Управление здоровьем населения	Для информирования лиц или процессов, ответственных за мониторинг населения и групп населения на предмет событий в сфере здравоохранения, тенденций и результатов с целью информирования по значимым стратегиям и политикам
10	Исследование	Для поддержки получения обобщенных знаний
11	Исследования рынка	Для поддержки получения знаний, характерных для продукта или организации
12	Судебные процедуры	Для информирования лиц или процессов, ответственных за обеспечение соответствия законодательству или законно уполномоченное ведение расследований по уголовным, гражданским и нормативным правонарушениям
13	Назначения субъекта получения медицинской помощи	Для информирования субъекта получения медицинской помощи или его/ее законно уполномоченного агента по поддержке интересов субъекта получения медицинской помощи или в случае смерти для поддержки ухода за членом семьи
14	Точно не установленное	Раскрытие на основе авторизаций, не требующих указания цели или целей, для которых не применимы другие категории в данном разделе

Логическое обоснование. Данное значение позволяет оценивать соответствие события аудита политике предоставления доступа в организации.

7.4 Идентификация точки доступа

7.4.1 Код типа точки доступа к сети (Network access point type code)

Описание. Идентификатор для типа точки доступа к сети, создавшей событие аудита.
Степень важности. Необязательное.
Формат/Значения. Перечисление, как показано в таблице 10.

Таблица 10 — Коды типа точки доступа

Значение	Содержание
1	Имя машины, включая имя DNS
2	IP-адрес
3	Номер телефона

Логическое обоснование. Эти данные определяют идентификатор типа точки доступа к сети прибора пользователя для события аудита. Это необязательное значение, которое может быть использовано для групповых событий, записанных на отдельных серверах, для анализа доступа в соответствии с типом точки доступа к сети.

7.4.2 Идентификатор точки доступа к сети (Network access point ID)

Описание. Идентификатор для точки доступа к сети прибора пользователя для события аудита. Это может быть идентификатор прибора, IP-адрес или какой-либо другой идентификатор, ассоциированный с прибором.

Степень важности. Необязательное.

Формат/Значения. Если установлено, текст может быть ограничен до допустимых значений для данного типа точки доступа к сети. В случае нескольких доступных вариантов рекомендации должны быть максимально индивидуальными.

Логическое обоснование. Эти данные определяют точку доступа к сети пользователя, которая может отличаться от сервера, осуществившего действие. Это необязательное значение, которое может быть использовано для групповых событий, записанных на отдельных серверах, для анализа доступа к данным определенной точки доступа к сети во всех серверах.

Примечание — Идентификатор точки доступа к сети не заменяет личную учетность. В частности, IP-адреса в интернете очень изменчивы и могут быть присвоены нескольким людям за короткий период времени.

Примеры

1 Идентификатор точки доступа к сети: 192.0.2.2.

Код типа точки доступа к сети: 2 = IP-адрес.

2 Идентификатор точки доступа к сети: 610-555-1212.

Код типа точки доступа к сети: 3 = Номер телефона.

7.5 Идентификация источника аудита

7.5.1 Общие сведения

Данные следов аудита могут быть собраны из различных источников, таких как:

- данные защиты информационных систем;
- службы каталогов;
- сервисы определения политик доступа;
- данные доступа на уровне приложения.

Защищенные сервисы должны получать эти данные.

Рассматриваемые ниже данные необходимы в основном для систем и процессов приложений. Так как многоуровневые, распределенные или составные приложения делают идентификацию источника неоднозначной, данный набор полей может повторяться для каждого приложения или процесса, активно участвующего в событии. Например, множественные наборы значений могут идентифицировать участвующие веб-серверы, процессы приложений и серверные потоки баз данных в n-уровневом распределенном приложении. Неактивные участники события, например средства передачи данных сетей низкого уровня, должны быть идентифицированы.

В зависимости от стратегий внедрения, возможно, что компоненты в многоуровневом, распределенном или составном приложении могут создавать несколько записей аудита для одного события приложения. Различные данные в записи аудита могут быть использованы для идентификации таких случаев, поддерживая последующее сокращение объема данных. Настоящий стандарт предполагает, что механизмы хранения и представления отчетов осуществляют сокращение объема данных при необходимости, но не определяет, какие это механизмы.

7.5.2 Идентификатор объекта предприятия аудита (Audit enterprise site ID)

Описание. Местоположение источника логического объекта в пределах сети предприятия, например больницы или другого местоположения в пределах группы провайдера, осуществляющего поддержку нескольких компаний.

Степень важности. Условно обязательное.

Формат/Значения. Текстовая строка уникального идентификатора в пределах предприятия здравоохранения. Является необязательной, если система аудита уникально определена Идентификатором источника аудита.

Логическое обоснование. Данное значение помогает различать объекты в информационной системе расположенного в нескольких местах предприятия.

Примечание — Значение определяется приложением, создающим запись аудита. Оно содержит уникальный код, который идентифицирует организацию (владельца данных), которая известна предприятию. Далее значение квалифицирует и однозначно определяет Идентификатор источника аудита. Значения могут различаться в зависимости от типа деятельности. В пределах организации могут существовать уровни дифференциации.

7.5.3 Идентификатор источника аудита (Audit source ID)

Описание. Идентификатор источника создания события.

Степень важности. Обязательное.

Формат/Значения. Текстовая строка уникального идентификатора, по крайней мере, в пределах Идентификатора объекта предприятия аудита.

Логическое обоснование. Данное поле привязывает событие к определенной системе источника. Оно может быть использовано для групповых событий для анализа в соответствии с тем, где произошло событие.

7.5.4 Код типа источника аудита (Audit source type code)

Описание. Код, определяющий тип источника создания события.

Степень важности. Необязательное.

Формат/Значения. Перечисление закодированных значений, либо определенных разработчиками системы, либо упоминаемое в словаре стандарта. Если значение не определено или не упоминается в стандарте, то значения по умолчанию для атрибута «code» соответствуют указанным в таблице 11.

Таблица 11 — Коды типа источника аудита

Значение	Содержание
1	Интерфейс конечного пользователя
2	Прибор или инструмент для получения данных
3	Уровень процесса веб-сервера в многоуровневой системе
4	Уровень процесса сервера приложения в многоуровневой системе
5	Уровень процесса сервера базы данных в многоуровневой системе
6	Сервер безопасности, например контроллер доменов
7	Компонент сети 1—3 уровней по ИСО
8	Системное программное обеспечение уровней 4—6 по ИСО
9	Внешний источник, другой или неизвестный

Схема XML в RFC 3881 определяет дополнительные атрибуты для определенных реализацией закодированных значений или значений, упоминаемых в стандартах, представленных в таблице 12.

Таблица 12 — Ссылочные атрибуты Кода идентификатора роли

Атрибут	Значение
CodeSystem	Ссылка на OID
CodeSystemName	Имя системы кодирования; настоятельно рекомендуется учитывать для локально определенных кодовых наборов

Окончание таблицы 12

Атрибут	Значение
DisplayName	Значение, которое должно быть использовано при демонстрации и в отчетах
OriginalText	Входное значение, которое было переведено в код

Источники аудита могут быть классифицированы более чем одним способом, поэтому могут быть обозначены различные значения.

Логическое обоснование. Данное поле показывает, какой тип источника обозначается Идентификатором источника аудита. Это необязательное значение, которое может быть использовано для групповых событий для анализа в соответствии с типом источника происхождения события.

7.6 Идентификация объекта-участника

7.6.1 Общие сведения

Объекты события, проверяемые аудитом, считаются объектами-участниками. Следующие данные помогают процессу аудита посредством обозначения особых случаев данных или объектов, к которым осуществлялся доступ.

Эти данные необходимы, если значений для Идентификации события, Идентификации активного участника и Идентификации источника аудита не достаточно, чтобы задокументировать все событие, проверяемое аудитом. Производственные записи аудита, содержащие эти данные, могут быть разрешены или запрещены, как установлено политикой организации здравоохранения и нормативными требованиями.

События могут иметь несколько объектов-участников, поэтому данная группа может быть повторяющимся набором значений. Например, в зависимости от политики учреждения и выбора метода внедрения:

- два набора значений объекта-участника могут быть использованы для определения доступа к персональной медицинской информации по номеру медицинской карты и по определенному обращению или случаю медицинской помощи субъекта получения медицинской помощи;
- объект получения медицинской помощи и его уполномоченный представитель могут быть определены одновременно;
- лечащий врач и консультирующие направленные лица могут быть определены одновременно;
- все субъекты получения медицинской помощи, определенные в рабочем списке, могут быть идентифицированы.

В некоторых случаях (например, рентгенологические исследования или передачи большого числа документов в формате архитектуры общих данных HL7) может быть определен набор связанных объектов-участников, определенных учетным номером или номером исследования. Однако следует отметить, что каждая запись аудита документирует только один случай использования таких отношений объекта-участника и не служит для документирования всех отношений, которые могут происходить или быть возможными.

7.6.2 Код типа объекта-участника (Participant object type code)

Описание. Код для типа объекта-участника, проверяемого аудитом. Данное значение отличается от роли пользователя или отношения любого пользователя с объектом-участником.

Степень важности. Обязательное.

Формат/Значения. Перечисление, как показано в таблице 13.

Таблица 13 — Коды типа объекта-участника

Значение	Содержание
1	Лицо
2	Объект системы
3	Организация
4	Другое

Логическое обоснование. Для описания объекта, над которым производится действие. В дополнение к запросам по предмету действия в событии, проверяемом аудитом, также важно иметь возможность делать запрос по типу объекта для действия.

7.6.3 Роль кода типа объекта-участника (Participant object type code role)

Описание. Код, представляющий функциональную роль приложения объекта-участника, проверяемого аудитом.

Степень важности. Обязательное.

Формат/Значения. Перечисление, характерное для Кода типа объекта-участника, как показано в таблице 14.

Таблица 14 — Коды ролей объекта-участника

Значение	Содержание	Коды типа объекта-участника
1	Субъект получения медицинской помощи	1 — Лицо
2	Местоположение	3 — Организация
3	Сегмент EHR	2 — Объект системы
4	Ресурс	1 — Лицо 3 — Организация
5	Основной файл	2 — Объект системы
6	Пользователь	1 — Лицо 2 — Объект системы (пользователь-не человек)
7	Список	2 — Объект системы
8	Работник здравоохранения	1 — Лицо
9	Абонент	3 — Организация
10	Гарант	1 — Лицо 3 — Организация
11	Запись защиты пользователя	1 — Лицо 2 — Объект системы
12	Группа защиты пользователя	2 — Объект системы
13	Ресурс защиты	2 — Объект системы
14	Определение степени детализации защиты	2 — Объект системы
15	Поставщик	1 — Лицо 3 — Организация
16	Адресат данных	2 — Объект системы
17	Хранилище данных	2 — Объект системы
18	Расписание	2 — Объект системы
19	Клиент	3 — Организация
20	Задание	2 — Объект системы
21	Поток заданий	2 — Объект системы
22	Таблица	2 — Объект системы
23	Критерии маршрутизации	2 — Объект системы
24	Запрос	2 — Объект системы

«Ресурс защиты» является абстрактным защищаемым объектом, например экраном, интерфейсом, документом, программой и т. д. или даже журналом аудита или хранилищем.

Логическое обоснование. Иногда для подробного анализа аудита может быть необходимо обозначить более структурированный тип участника, основываясь на роли в приложении, которую он играет.

7.6.4 Жизненный цикл данных объекта-участника (Participant object data life cycle)

Описание. Идентификатор для этапа жизненного цикла данных для объекта-участника. Может использоваться для предоставления аудиторских следов для данных через некоторое время, когда они проходят через систему.

Степень важности. Необязательное.

Формат/Значения. Перечисление, как показано в таблице 15.

Таблица 15 — Коды этапов объекта-участника

Значение	Содержание
1	Ввод/ Создание
2	Импорт/ Копирование оригинала
3	Поправка
4	Проверка
5	Перевод
6	Доступ/ Использование
7	Повторная идентификация
8	Агрегирование, суммирование, получение
9	Отчет
10	Экспорт/ Копирование
11	Раскрытие
12	Получение или раскрытие
13	Архивирование
14	Логическое удаление
15	Постоянное стирание/ Физическое уничтожение
16	Повторная классификация

Логическое обоснование. Политики предприятий по конфиденциальности и защите могут дополнительно подпадать под разные правила учетности в зависимости от жизненного цикла данных, что обеспечивает различающиеся значения для таких случаев.

7.6.5 Код типа идентификатора объекта-участника (Participant object ID type code)

Описание. Описывает идентификатор, содержащийся в Идентификаторе объекта-участника.

Степень важности. Обязательное.

Формат/Значения. Перечисление закодированных значений, характерных для Кода типа объекта-участника с использованием атрибута-имени «code». Коды, данные в таблице 16, являются стандартным набором.

Таблица 16 — Коды типов идентификатора объекта-участника

Значение	Содержание	Коды типа объекта-участника
1	Идентификатор медицинской записи	1 — Лицо
2	Идентификатор субъекта получения медицинской помощи	1 — Лицо
3	Идентификатор контакта	1 — Лицо

Окончание таблицы 16

Значение	Содержание	Коды типа объекта-участника
4	Идентификатор страхования пациента	1 — Лицо
5	Национальный персональный идентификатор для медицинских услуг (например, номер социального страхования)	1 — Лицо
6	Идентификатор счета	1 — Лицо 3 — Организация
7	Идентификатор гаранта	1 — Лицо 3 — Организация
8	Имя отчета	2 — Объект системы
9	Идентификатор отчета	2 — Объект системы
10	Критерии поиска	2 — Объект системы
11	Идентификатор системы пользователя	1 — Лицо 2 — Объект системы
12	Универсальный идентификатор ресурса (URI)	2 — Объект системы
13	Идентификатор объекта (например, идентификатор записи, идентификатор лабораторного испытания и т. д.)	2 — Объект системы

Текстовые строки Идентификатора пользователя и URI [RFC2396] предназначены для использования для событий срабатывания системы администрирования защиты с целью идентификации объектов, над которыми осуществляется действие.

Коды могут быть стандартным набором, указанным выше, определенными реализацией или могут ссылаться на стандартное словарное перечисление, таким как типы носителей, определенные в таблице 207 стандарта HL7, версия 2.4, или в ИСО 12052 (DICOM) [1].

Схема XML в RFC 3881 определяет дополнительные атрибуты для определенных реализацией закодированных значений или значений, упоминаемых в стандартах, представленные в таблице 17.

Таблица 17 — Ссылочные атрибуты Кода идентификатора объекта-участника

Атрибут	Значение
CodeSystem	Ссылка на OID
CodeSystemname	Имя системы кодирования; настоятельно рекомендуется учитывать для локально определенных кодовых наборов
DisplayName	Значение, которое должно быть использовано при демонстрации и в отчетах
OriginalText	Входное значение, которое было переведено в код

Логическое обоснование. Требуется для установления различия различных идентификаторов, которые синонимично идентифицируют объект-участник.

7.6.6 Комплекс политик доступа объекта-участника (Participant object permission PolicySet)

Описание. Указатель на политики, которые руководят доступом к Идентификатору объекта-участника.

Степень важности. Необязательное.

Формат/Значения. Значения являются зависимыми от организации и реализации текстовыми строками.

7.6.7 Чувствительность объекта-участника (Participant object sensibility)

Описание. Обозначает определенную политикой чувствительность для Идентификатора объекта-участника, такую как VIP, ВИЧ-статус, состояние психического здоровья или схожие темы.

Степень важности. Необязательное.

Формат/Значения. Значения являются зависимыми от организации и реализации текстовыми строкам.

7.6.8 Идентификатор объекта-участника (Participant object ID)

Описание. Обозначает особый случай объекта-участника.

Степень важности. Обязательное.

Формат/Значения. Текстовая строка. Формат значений зависит от Кода типа объекта-участника и Кода типа идентификатора объекта-участника.

Логическое обоснование. Данное поле определяет определенный экземпляр объекта, такой как субъект получения медицинской помощи, для распознавания/отслеживания проблем конфиденциальности и защиты.

Примечание — Данный идентификатор считается основным уникальным ключом идентификатора для объекта, так, чтобы при внедрении он мог быть составным полем данных.

7.6.9 Имя объекта-участника (Participant object name)

Описание. Характерный для отдельного случая дескриптор Идентификатора объекта-участника, проверяемого аудитом, например, имя человека.

Степень важности. Необязательное.

Формат/Значения. Текстовая строка.

Логическое обоснование. Данное поле может использоваться в запросе/отчете для идентификации событий аудита по определенному человеку, например, там, где были использованы синонимичные Идентификаторы объекта-участника (идентификатор субъекта получения медицинской помощи, идентификатор медицинской записи, идентификатор контакта и т. д.).

7.6.10 Запрос объекта-участника (Participant object query)

Описание. Действительный запрос для объекта участника типа запрос.

Степень важности. Необязательное.

Формат/Значения. Данные, закодированные посредством метода кодирования информации в 64-разрядный код.

Захватить фактический вход вопроса к процессу вопроса.

Логическое обоснование. Для событий запроса может потребоваться захватить фактический ввод запроса d процесса запроса с целью идентификации конкретного события. Ввиду различий в реализации запросов и кодирования данных для них этот запрос является двоичным объектом данных, закодированных методом кодирования информации в 64-разрядный код. Далее он может быть раскодирован или интерпретирован при последующей обработки анализа аудита.

7.6.11 Подробные данные об объекте-участнике (Participant object detail)

Описание. Зависимые от реализации данные о конкретных подробных данных об объекте, к которому осуществлялся доступ, или который был использован.

Степень важности. Необязательное.

Формат. Пара тип-значение. Атрибут «type» («тип») является зависимой от реализации текстовой строкой. Атрибут «value» («значение») является данными, закодированными посредством метода кодирования информации в 64-разрядный код.

Логическое обоснование. В конкретных аудируемых реализациях могут потребоваться конкретные детали или значения объекта, к которому был осуществлен доступ. Пара тип-значение позволяет использовать зависимые от реализации и локально распространенные идентификаторы и значения типа объекта. Например, объект клинической диагностики может содержать несколько результатов испытаний, и этот элемент может задокументировать тип и количество результатов.

Для этих элементов возможны различные кодировки данных, поэтому значение является двоичным объектом данных, закодированных методом кодирования информации в 64-разрядный код. Далее он может быть раскодирован или интерпретирован посредством последующей обработки анализа аудита.

8 Записи аудита для отдельных событий

8.1 События доступа

Данная запись аудита, как показано в таблице 18, описывает создание, чтение, изменение и удаление персональной медицинской информации.

Таблица 18 — Формат записей аудита для событий доступа

Категория	Имя поля	Опция	Ограничение значений
Связанное с событием	EventID	M	Идентификатор события, проверяемого аудитом
	EventActionCode	M	Тип действия, выполненного во время события, которое привело к созданию журнала аудита. Установлены следующие значения: EV: “C” (Создать), “R” (Прочитать), “U” (Обновить), “D” (Удалить)
	EventDateTime	M	Дата/время наступления события
	EventOutcomeIndicator	U	Код для обозначения успеха (или неудачи) события
	EventTypeCode	U	Тип события
Связанное с пользователем (1..2)	UserID	M	Идентификатор пользователя или процесса, обрабатывающего данные. Если известны и пользователь, и процесс, то должны быть включены оба. Это уникальное значение в источнике аудита (AuditSourceID)
	AlternateUserID	U	Альтернативный идентификатор пользователя или процесса, обрабатывающего данные
	UserName	U	Имя пользователя или процесса, обрабатывающего данные
	UserIsRequestor	U	Данное значение показывает, являются ли пользователь или процесс, обрабатывающий данные, инициаторами запроса данного события. Установлено следующее значение: EV TRUE
	RoleIDCode	U	Роль, которую играют пользователь или процесс, обрабатывающие данные, при исполнении события
	PurposeOfUse	U	Код, обозначающий цель использования данных, к которым осуществлен доступ
	NetworkAccessPointTypeCode	U	Код типа точки доступа к сети
	NetworkAccessPointID	U	Идентификатор точки доступа к сети
Связанное с системой источника происхождения (1)	AuditEnterpriseSiteID	U	Логическое расположение системы источника происхождения. Используется для изменения поля AuditSourceID
	AuditSourceID	M	Уникальный идентификатор системы источника происхождения
	AuditSourceTypeCode	U	Код типа системы источника происхождения

Окончание таблицы 18

Категория	Имя поля	Опция	Ограничение значений
Связанное с объектом-участником (информация о пациенте, к которому осуществлялся доступ) (1)	ParticipantObjectTypeCode	M	Код типа объекта-участника. Установлено следующее значение: EV1 (человек)
	ParticipantObjectTypeCodeRole	M	Код роли объекта-участника. Установлено следующее значение: EV 1 (пациент)
	ParticipantObjectDataLifeCycle	U	Идентификатор этапа жизненного цикла для объекта-участника
	ParticipantObjectIDTypeCode	M	Код типа, содержащегося в объекте-участнике. Установлено следующее значение: EV 2 (Идентификатор пациента)
	ParticipantObjectPolicySet	U	Действующий комплекс политик доступа для Идентификатора объекта-участника, например информация о согласии пациента
	ParticipantObjectSensitivity	U	Чувствительность, определенная политикой для Идентификатора объекта-участника
	ParticipantObjectID	M	Идентификатор частного случая объекта-участника. Идентификатор пациента установлен
	ParticipantObjectName	U	Имя объекта-участника. Имя субъекта получения медицинской помощи установлено
	ParticipantObjectDetail	U	Подробная информация по частному случаю объекта-участника
Связанное с объектом-участником (информация о сегменте EHR, к которому осуществлялся доступ) (1..N)	ParticipantObjectTypeCode	M	Код типа объекта-участника. Установлено следующее значение: EV 2 (объект системы)
	ParticipantObjectTypeCodeRole	M	Код роли объекта-участника. Установлено следующее значение: EV 3 (сегмент EHR)
	ParticipantObjectDataLifeCycle	U	Идентификатор этапа жизненного цикла для объекта-участника
	ParticipantObjectIDTypeCode	M	Код типа, содержащегося в объекте-участнике. Установлено следующее значение: EV 13 (Идентификатор объекта)
	ParticipantObjectPolicySet	U	Действующий комплекс политик доступа для Идентификатора объекта-участника
	ParticipantObjectSensitivity	U	Чувствительность, определенная политикой для Идентификатора объекта-участника
	ParticipantObjectID	M	Идентификатор частного случая объекта-участника. Идентификатор сегмента EHR установлен
	ParticipantObjectName	U	Имя объекта-участника. Имя сегмента EHR установлено
	ParticipantObjectDetail	U	Подробная информация по частному случаю объекта-участника

8.2 События запроса

Данная запись аудита, как показано в таблице 19, описывает отправление и получение запроса. В ней регистрируется не ответ на запрос, а только факт отправления запроса.

Таблица 19 — Формат записей аудита для событий запроса

Категория	Имя поля	Опция	Ограничение значений
Связанное с событием	EventID	M	Идентификатор события аудита
	EventActionCode	M	Тип действия, выполненного во время события, которое привело к созданию журнала аудита. Установлено следующее значение: EV: “E” (Выполнить)
	EventDateTime	M	Дата/время наступления события
	EventOutcomeIndicator	U	Код для обозначения успеха (или неудачи) события
	EventTypeCode	U	Тип события
Связанное с запрашивающим лицом (1)	UserID	M	Процесс, обрабатывающий данные. Это уникальное значение в источнике аудита (AuditSourceID)
	AlternateUserID	U	Альтернативный идентификатор пользователя или процесса, обрабатывающего данные
	UserName	U	Имя процесса, обрабатывающего данные
	UserIsRequestor	U	Данное значение показывает, являются ли пользователь или процесс, обрабатывающий данные, инициатором запроса данного события
	RoleIDCode	U	Роль, которую играют пользователь или процесс, обрабатывающие данные, при исполнении события
	PurposeOfUse	U	Код, обозначающий цель использования данных, к которым осуществлен доступ
	NetworkAccessPointTypeCode	U	Код типа точки доступа к сети
	NetworkAccessPointID	U	Идентификатор точки доступа к сети
Связанное с вышеуказанным вопросом (1)	UserID	M	Идентификатор процесса, отвечающего на запрос. Это уникальное значение в источнике аудита (AuditSourceID)
	AlternateUserID	U	Альтернативный идентификатор процесса, отвечающего на запрос
	UserName	U	Имя процесса, отвечающего на запрос
	UserIsRequestor	U	Данное значение показывает, является ли процесс, отвечающий на запрос, инициатором запроса данного события
	RoleIDCode	U	Код роли, которую играет процесс, обрабатывающий данные во время исполнения
	NetworkAccessPointTypeCode	U	Код типа точки доступа к сети
	NetworkAccessPointID	U	Идентификатор точки доступа к сети

Окончание таблицы 19

Категория	Имя поля	Опция	Ограничение значений
Связанное с альтернативным участником (1..2)	UserID	M	Идентификатор участника, с которым установлена связь и который является известным. В особенности пользователя или процесса, являющегося инициатором запроса. Это уникальное значение в источнике аудита (AuditSourceID)
	AlternateUserID	U	Альтернативный идентификатор альтернативного участника
	UserName	U	Альтернативное имя альтернативного участника
	UserIsRequestor	U	Данное значение показывает, является ли альтернативный участник инициатором запроса данного события.
	RoleIDCode	U	Роль альтернативного участника
	NetworkAccessPointTypeCode	U	Код типа точки доступа к сети
	NetworkAccessPointID	U	Идентификатор точки доступа к сети
Связанное с системой источника происхождения (1)	AuditEnterpriseSiteID	U	Логическое расположение системы источника происхождения. Используется для изменения поля AuditSourceID
	AuditSourceID	M	Уникальный идентификатор системы источника происхождения
	AuditSourceTypeCode	U	Код типа системы источника происхождения
Связанное с объектом-участником (содержание запроса) (1)	ParticipantObjectTypeCode	M	Код типа объекта-участника. Установлено следующее значение: EV 2 (система)
	ParticipantObjectTypeCodeRole	M	Код роли объекта-участника. Установлено следующее значение: EV 3 (отчет)
	ParticipantObjectDataLifeCycle	U	Идентификатор этапа жизненного цикла для объекта-участника
	ParticipantObjectIDTypeCode	M	Код типа, содержащегося в поле ParticipantObjectID. Установлено следующее значение: EV 10 (формула запроса)
	ParticipantObjectPolicySet	U	Действующий комплекс политик доступа для поля ParticipantObjectID
	ParticipantObjectSensitivity	U	Чувствительность, определенная политикой для поля ParticipantObjectID
	ParticipantObjectID	M	Идентификатор частного случая объекта-участника
	ParticipantObjectName	U	Имя объекта-участника
	ParticipantObjectQuery	M	Содержание запроса для объекта-участника, закодированное методом кодирования информации в 64-разрядный код. Это содержание должно быть проанализировано поставщиком-разработчиком
	ParticipantObjectDetail	U	Подробная информация по частному случаю объекта-участника

9 Защищенное управление данными аудита

9.1 Меры предосторожности

Для поддержания конфиденциальности и целостности медицинских карт, а также целостности и доступности систем медицинской информации в IETF RFC 3881 указаны следующие критерии:

Данные аудита должны быть защищены, по крайней мере, в той же степени, что и основные данные и действия, проверяемые аудитом. В защиту входит контроль доступа, а также функции обеспечения целостности данных и функции восстановления данных. Данный документ допускает, но не указывает на необходимость в политиках и технических методах осуществления защиты.

Можно допустить, что данные аудита могут подвергаться использованию не по назначению, например, отслеживанию частоты и характера использования системы для измерения производительности. Стандарт ASTM E2147-01 [10] в п. 5.3.10 устанавливает: «Запретить использовать по причинам, отличным от обеспечения осуществления защиты и выявления пробелов в защите в информационных системах медицинских карт, например, аудиты не должны использоваться для изучения профилей деятельности или профилей движения сотрудников».

Управление записями аудита должно соответствовать ИСО 15489-1 [3] по управлению записями. Требования защищенности для архивирования записей аудита схожи с требованиями по архивированию электронных медицинских карт, указанных в ИСО/ТС 21547 [5].

Руководство по долгосрочному архивированию при соответствии руководству обеспечения целостности данных также дано в IETF RFC 4810 и IETF RFC 4998.

Особое внимание следует уделить защите распределенных следов аудита. В то время как электронные медицинские карты могут быть распределены среди множества информационных систем и охватывать отдельные предметные области политики защищенности, это так же относится и к аудиторским следам. Должна поддерживаться защищенность логических аудиторских следов.

9.2 Обеспечение доступности системы аудита

Система аудита должна обеспечивать достаточный объем мер для того, чтобы гарантировать, что в аудиторский след вносятся записи вне зависимости от того, когда используется система медицинской информации.

Система аудита должна документировать все случаи, когда аудиторский след не работал, был выключен или не функционировал из-за сбоя системы.

Система аудита должна показывать или сообщать, какие аудиты включены/выключены в заданное время.

9.3 Требования к хранению

Организация, ответственная за поддержание работы журнала аудита, должна определить политику хранения, руководящую записями аудита.

Хранение записей аудита должно соответствовать законодательным требованиям и соответствующим политикам.

Хранение записей аудита должно поддерживать наличие медицинских записей, данных и документов.

9.4 Обеспечение конфиденциальности и целостности следов аудита

Система аудита должна обеспечивать достаточный объем мер для защиты журналов аудита от несанкционированного доступа. В частности, она должна:

a) обеспечивать доступ к записям аудита;

b) защищать доступ к системным инструментам аудита для предотвращения злоупотребления и несанкционированного доступа;

c) отслеживать все действия со следами аудита, посредством защищенного журнала, в котором указывается время, действие и исполнитель действия;

d) документировать все случаи, когда аудиторский след не работал, был выключен или не функционировал из-за отказа системы и

e) сообщать, какие аудиты включены/выключены в заданное время.

9.5 Доступ к данным аудита

Доступ к данным аудита должен тщательно контролироваться и сам должен подлежать проверке аудитом. Доступ должен осуществляться подходящей информационной системой, способной обеспечивать осуществление этого контроля, а не самим аудиторским следом.

Средства осуществления аудита должны позволять анализ аудиторских следов по одному из закодированных или названных полей, определенных в разделе 7, с указанием даты/времени, по отдельности (где это возможно) или же в сочетании (например, все случаи осуществления доступа пользователем X, все события «delete» («удаление»), осуществленные пользователями роли Y, все события с участием субъекта получения медицинской помощи Z за прошедший месяц и т. д.).

В некоторых случаях пользователь аудита может получить доступ к источникам информации в дополнение к аудиторским следам, например для обнаружения шаблонов поведения (например, все поиски детей, выполненные пользователем, не являющимся педиатром и не связанным с педиатрией).

Приложение А
(справочное)

Сценарии аудита

А.1 Общие сведения

Существует много типов аудита: аудит защиты, аудит конфиденциальности, экспертный аудит, аудит выделения ресурсов, аудит производительности системы, аудит производительности сети, аудит управления конфигурацией, аудит обнаружения проникновения и т. д. данное приложение описывает различные сценарии использования журналов аудита.

А.2 Случай недовольной знаменитости

Пока в больнице находится знаменитость, кто-то из персонала, зная о статусе знаменитости субъекта получения медицинской помощи, использует информационную систему, связанную с уходом за больным, чтобы узнать номер палаты субъекта получения медицинской помощи и информацию из медицинской карты, и продает ее в газету или частному лицу.

Субъект получения медицинской помощи, обнаружив свое фото на обложке известной газеты, жалуется должностному лицу, ответственному за обеспечение конфиденциальности. Должностное лицо, ответственное за обеспечение конфиденциальности, использует хранилище данных аудита для просмотра всех случаев доступа к медицинской карте субъекта получения медицинской помощи и обнаруживает, что один случай произошел за пределами предусмотренного графиком времени проверки. В то время работали две медсестры, и после определенного расследования одна из них созналась, и ей был объявлен выговор.

Данный сценарий зависит от ведения записей аудита, а также от процесса выполнения аудита деятельности, которая была записана. Он должен включать в себя:

- создание записи/журнала аудита;
- передача (включая ожидание в очереди и локальные области хранения) записи/журнала аудита в хранилище;
- получение записи/журнала аудита;
- хранение записи/журнала аудита;
- аудит осуществления запросов/поисков для определения того, что произошло.

Это, в свою очередь, требует:

- поиск по соответствию даты и
- системы аудита, которые, по меньшей мере:
  - идентифицируют каждого пользователя, который, согласно отчетам, просматривал карту данного субъекта получения медицинской помощи,
  - идентифицируют каждый случай доступа данного пользователя к карте любого субъекта получения медицинской помощи и
  - идентифицируют каждый случай доступа узла к карте субъекта получения медицинской помощи;
- соответствие с RFC 3881 для обеспечения возможности поиска;
- соответствие с ИСО 12052 [1] (DICOM) в случае аудита технологического процесса рентгенологического исследования.

Вышеуказанный сценарий охватывает ряд возможных случаев для субъектов получения медицинской помощи с конкретными потребностями в аудите:

- субъекты получения медицинской помощи, в случае которых злоумышленник был серьезно мотивирован, например, объект получения медицинской помощи, который, сам того не желая, подвергается преследованию;
- жертва насилия:
  - объект получения медицинской помощи уведомляет должностное лицо, ответственное за обеспечение конфиденциальности, о необходимости закрыть доступ к персональной медицинской информации путем использования для этой информации маркировки, отличной от маркировки, используемой для идентификации VIP пациентов (у администрации может быть стандартный набор маркировок для идентификации данных такого типа субъектов). Для аудита в данном случае не стоит записывать, что объект получения медицинской помощи является «жертвой насилия», а скорее стоит записать, что должностному лицу, ответственному за обеспечение конфиденциальности, или должностному лицу, ответственному за обеспечение защищенности был отправлен сигнал о нарушении. Нам необходимо записать «код» данного нарушения, а не явно идентифицировать его простым текстом в записи аудита.

Для аудита можно стандартизировать:

- категории сигналов тревоги системы защиты — необходим механизм отправки сигналов тревоги. Можно применить сигнал тревоги для сценария возможного преследования/незаконной деятельности, а также более мощные сигналы для сценариев, рассмотренных ниже;

- коды и доверие к приложению для выявления шаблонов поведения;
- применение политики для выполнения обработки данных аудита, где политика определяет, когда и по какому поводу подавать сигнал;
- необходимость в использовании следующей функциональности из системного журнала: выборочная отправка журналов, которые соответствуют определенным (простым) шаблонам поведения в отдельное приложение, которое не является частью основного сервиса аудита. Это другое приложение-«наблюдатель» будет «смотреть» за плохим поведением и посылать сигналы (такой тип приложения также можно использовать для проблем с оборудованием);
- способность к извлечению основных данных из архива аудита;
- дополнительную возможность — добавить подключаемую программу для определенных видов поиска в хранилище данных аудита, но как минимум предоставить возможность вывести все данные из базы данных аудита на печать, чтобы иметь возможность проводить анализ вручную на этапе 1.

Сервис уведомлений может быть простым или сложным, но он должен знать, что куда посылать. Сервис уведомлений может быть условно зависимым сервисом. Существует два варианта этого случая, а именно:

Субъект получения медицинской помощи высокого уровня и злоумышленник *слабо* мотивирован.

Начальные условия угрозы. Злоумышленник, нацеленный на субъекта получения медицинской помощи, не имеет хорошего финансирования или стимула, т. е. злоумышленник не будет долго подкупать сотрудника или находиться в учреждении как сотрудник, а он непосредственно выполнит запросы в базу данных. В таких случаях ищут только неправомерные «нормальные» транзакции. Хранилище данных аудита должно позволять делать запросы случаев доступа по IP, PID, пользователю, промежутку времени и т. д.

Субъект получения медицинской помощи высокого уровня и злоумышленник серьезно мотивирован.

Злоумышленники для получения информации используют возможности запроса в основные базы данных, а не только основные функции поиска интерфейса хранилища (например, средства администраторов баз данных).

Требуемая функциональность. Запрос в журналы аудита по идентификатору субъекта получения медицинской помощи, по времени доступа и идентификатору пользователя, общий анализ хранилища.

Хранилище данных аудита должно быть способно сбросить (в сервис отчетов) записи аудита для соответствующего PID, идентификатора системы, временного окна и т. д.

Сервис отчетов получит из хранилища закодированную информацию и отобразит отчет в любом выбранном виде (предпочтительно пригодном для использования).

Требуемый интерфейс (куда хранилище данных аудита должно отправить сообщение, которое будет понятно сервису отчета и сервису анализа) (в случае, если к хранилищу подключен этот интерфейс) имеет четыре уровня:

a) события, связанные с конкретным субъектом получения медицинской помощи: нет необходимости просматривать любые запросы, просто ответь, есть ли события аудита, связанные с данным субъектом получения медицинской помощи;

b) покажи запросы, которые, как известно, вернули бы данные о субъекте получения медицинской помощи, даже если идентификатор субъекта не указан: детерминированные запросы / запросы, не учитывающие время (такие как запросы, хранящиеся в XDS);

c) покажи все события, удовлетворяющие диапазонам значений нескольких критериев: пользователь, временное окно, тип события и набор систем, представляющих интерес (например, все входы в систему и выходы из нее);

d) сложные запросы: пользовательские запросы, запросы по ИСО 12052 [1] (DICOM), запросы потока работ лаборатории, которые зависят от потока работ и требуют от запрашивающего знания состояния базы данных на момент осуществления запроса.

Уровни a), b) и c) могут осуществляться через прямой интерфейс к хранилищу.

Сервис анализа может быть использован для уровня d) и размещен сверху.

Возможная функциональность. Запрос в журналы аудита вручную или с использованием сервиса анализа.

Возможная новая область применения для аудита. Осуществление анализа/ сравнения/ связи между журналами планирования и журналами аудита для обнаружения незапланированных/ необычных случаев доступа.

Дополнительные сервисы. Хранилище запросов/сервис анализа для выяснения существуют ли необычные запросы?

А.3 Случай принудительно обеспеченного установленного в законодательном порядке права на неприкосновенность частной жизни (относящийся к прошлому, не активный)

В данном сценарии субъект получения медицинской помощи не хочет, чтобы его сосед, поставщик медицинской помощи, был осведомлен о его состоянии здоровья, субъект получения медицинской помощи может выдать своему врачу по оказанию первичной медицинской помощи разрешительный документ, постановляющий полностью закрыть доступ к его медицинской карте со стороны поставщика медицинских услуг. Через несколько недель должностное лицо, ответственное за обеспечение конфиденциальности врача по оказанию первичной медицинской помощи, получает сигнал о том, что сосед пытался получить доступ к картам, нарушая политику учреждения, и что в доступе было отказано. Должностное лицо, ответственное за обеспечение конфиденциальности, оповещает субъекта получения медицинской помощи о попытке получения доступа и о том, что она была неуспешной.

Обязательная функциональность. Формирование списка случаев доступа к медицинским картам через логин врача/ пользователя; формирование / демонстрация списка неуспешных попыток доступа; и формирование сигналов тревоги в момент, когда фиксируется событие, не уполномоченное разрешительными документами.

- Любой случай использования (низкого/ высокого уровня) требует возможности ретроспективного анализа аудита: «дайте мне данные, и я их проанализирую».
- Данный сценарий существует только для установления того, чтобы аудит мог быть «запрошен» по идентификатору процесса (PID), а также по успешным/ неуспешным результатам события.

Проблемы:

- в реальном мире существует множество случаев автоматизированной предварительной подкачки и кэширования данных. В большинстве транзакций поставщик или имя субъекта получения медицинской помощи указаны не в данных, а в информации связанного с ними приложения. Наглядный пример. Если человеку назначен прием, то его данные предварительно демонстрируются на экране в смотровом кабинете. Сервис аудита должен быть в состоянии сверять, кто был подключен к смотровому кабинету в то время, когда был назначен прием;
- неавторизованные попытки получить доступ, как указано выше, соседом поставщика медицинских услуг, должны либо отслеживаться приложением, либо проявляться как запросы от неожиданного источника;
- «сервис-наблюдатель» может иметь белый список смотровых кабинетов, которые могут предварительно просматривать данные и отправлять уведомление, если запрос поступает от неожиданного источника и/или в нарушение разрешительных документов или документов по получению доступа. Определение того, когда и по какому поводу сервис-наблюдатель оповещает, относится к вопросам местной политики.

А.4 Случай взломанного сервера

Недавно начал работать реестр состояния здоровья населения, и лицо, создавшее сервер, отказалось сменить пароль администратора. Некий хакер находит сервер и начинает использовать его, чтобы атаковать другие системы спамом от реестра состояния здоровья населения. Из-за необычно большого объема событий аудита и случаев доступа уровня администратора с неизвестного IP-адреса должностному лицу, ответственному за обеспечение защиты отправляется сигнал, и это лицо сразу же проверяет журналы аудита и понимает, что произошло, и может это прекратить. Дальнейший анализ журналов аудита обнаруживает некоторые дополнительные уязвимости, которые не были видны при установке системы, и производится усиление защиты для повышения защищенности системы.

Это другой тип сервиса приложения, а также другой тип аудита.

Эти записи аудита будет создавать защитная система. Журналы маршрутизатора не характерны для здравоохранения.

Обязательная функциональность. Необходимо «архитектурно» соответствовать тому, как профессиональная IT-индустрия решает эту проблему.

Факт отправления сигнала тревоги также подлежит аудиту.

А.5 Случай уполномоченного пользователя, который злоупотребляет этими полномочиями

Некое лицо просит своего партнера устроиться на работу в качестве регистрирующего агента в новой информационной Системе / Регистре поставщиков по лекарственным средствам и затем зарегистрировать это лицо и других лиц как врачей с правами электронного назначения, чтобы они могли незаконно назначать лекарственные средства.

Часто единственным способом раскрыть такой тип событий является естественная подозрительность или случайный анализ журналов аудита.

Как можно своевременно на это реагировать? Может ли аудит и мониторинг помочь обнаружить необычные случаи назначения подлежащих контролю лекарственных средств? (Резкий скачок в назначении морфина?) Наименьшее, чем может помочь система, — это немедленное предоставление доказательств несанкционированных регистраций при обнаружении пользователя, злоупотребляющего полномочиями, а также список всех «врачей», зарегистрированных при использовании учетной записи пользователя, злоупотребляющего полномочиями.

Обязательная функциональность. Формировать список успешных событий регистрации пользователя.

Дополнительная функциональность. Делать перекрестные ссылки между сервисом аудита и другими сервисами для определения области нарушения.

Потенциальная функциональность для сервиса *ID Mgmt*. Сверять личность в регистре поставщиков с учетными данными поставщиков.

А.6 Случай неправильно направленных результатов исследований

Субъект получения медицинской помощи ждал свои результаты лабораторных исследований уже в течение двух недель, когда врач сообщил ему, что при использовании новой информационной системы лаборатории результаты должны быть доступны менее чем через 48 часов. Когда субъект получения медицинской помощи звонит в офис своего врача, обнаруживается, что в офисе имеется запись о заказе результатов из лаборатории, но не сами результаты. Медсестра звонит в лабораторию и спрашивает, что случилось с результатами исследований. Лаборатория проверяет свои журналы аудита и находит номер полученного заказа результатов из лаборатории, а также результаты лабораторных испытаний, которые были отправлены в ответ. Лаборант проверяет, куда были

отправлены результаты и понимает, что результаты были отправлены в офис другого врача. Лаборант пересылает результаты правильному получателю, и проверяет ARR, чтобы убедиться, что результаты были повторно отправлены должным образом (успешный результат события и правильный получатель) и звонит медсестре, чтобы узнать, получила ли она их. Медсестра звонит субъекту получения медицинской помощи, чтобы сообщить ему, что результаты получены.

Некоторые дополнительные уточняющие данные должны быть добавлены в журналы аудита для поддержки этого сценария, такие как: номера для отслеживания заказа, номера отчетов и т. д. Необходимо будет установить баланс между добавлением в журналы слишком большого объема уточняющих данных и анализом, который может устанавливать связь между заказами с запросами в журнале аудита. Возникает вопрос о том, необходимо ли сделать это при помощи средств управления потоком работ или же при помощи журнала аудита? Рентгенология делает это по двум направлениям при помощи средств управления потоком работ (подтверждение отправки, получения и прочтения отчетов, а также номера контейнеров и т. д.). Предоставление отчетов при помощи средств управления потоком работ могут обрабатываться с помощью отдельного аудита — предоставление отчетов лаборатории и подтверждение БД. Интерфейс может обеспечить возможность согласования журналов отчетности лаборатории с другими журналами аудита в ходе расследований. Например, сервис сопоставления журналов.

Может существовать отчетность по потоку работ и сервис аудита в рамках информационной системы, будь то лаборатории назначения или радиология. Также должна учитываться интеграция с логистикой (доставка и т. д.).

Обязательная функциональность. Показывать события, а также отправителя и получателя.

Возможная функциональность. Результаты были отправлены в неправильное место из-за ошибки в реестре поставщиков и инцидент обнаружил необходимость исправления / обновления реестра поставщиков. Как эта необходимость корректирующих действий может автоматически срабатывать и решаться?

Этот сценарий отличается тем, что он не является ни мониторингом в реальном времени, ни управлением, а использованием системы аудита для проверки потока работ.

В данном сценарии есть некий пользователь, не являющийся администратором, который может использовать интерфейс хранилища данных аудита, который должен быть удобным и отличаться от обычного интерфейса.

В этом сценарии возникают следующие вопросы:

- может ли система определить, не потерялось ли сообщение?
- может ли система определить, не произошла ли операция? Так как операции являются событиями, подлежащими аудиту, эта информация должна быть получена;
- существует ли способ анализа наличия или отсутствия успешно или неуспешно отправленных сообщений?
- если появляется сообщение об ошибке (ошибка отклика), то оно может привязаться к сервису мониторинга, т. е. если система может это обнаружить, то сообщить о потере;
- для обнаружения несоответствий между полученными уведомлениями и отправленными уведомлениями существует функция сопоставления/ анализа, которая находится вне сферы действия настоящего стандарта.

Сотрудники службы безопасности также хотели бы знать: если надлежащий специалист не получил сообщение из лаборатории в нужное время, то получал ли сообщения кто-нибудь еще в это время?

Отчасти это сценарий потока работ / предоставления отчетов / производительности. Сервис аудита может передать эту возможность сервису потока работ.

А.7 Случай непредсказуемости операций

Системный администратор больницы замечает необычное количество неудачных операций. После проведения диагностики системы системный администратор может определить, что каждые несколько часов происходит огромный спад в пропускной способности, но не может определить почему. Администратор проверяет журналы и понимает, что приложение В посылает каждый заказ в лабораторию по два раза и, как следствие, происходит перегрузка системы.

Это случай администрирования системы и измерения производительности, такой как сценарий взломанного сервера. Информация, которая должна быть проверена аудитом, существенно отличается от примеров использования конфиденциальности и защищенности.

Общая система аудита может оставаться последовательной повсеместно и использовать те же возможности отправлять и хранить журналы. Информация, которая будет зарегистрирована и то, где она будет загружена, будет определяться местной политикой конфигурации.

Во-первых, это веб-сервис для ARR интерфейса, который говорит «возвращайте мне все, что покажется вам необычным», где необычное — это, например, «более пяти последовательных неудачных попыток или неудачных результатов операций».

В современном мире этот вид аудита осуществляется путем предоставления администратору возможности проанализировать поток необработанных данных при помощи наиболее общих инструментов.

Система может не дать аналитические данные для входящего потока аудита, но может дать доступ к необработанному потоку аудита через интерфейс в случае, если кто-то захочет осуществить его анализ.

Этот случай может быть расширен, включив такие переменные, как беспроводной мониторинг с использованием медицинских приборов и удаленный мониторинг объектами получения медицинской помощи.

А.8 Случай исчезающих записей аудита. Хранилище данных аудита как цель

Кто-то пытается скрыть свои следы. Во всех сервисах / системах должно быть установлено одно и то же время для того, чтобы заметить пробелы в данных, потому что для злоумышленника проще всего уничтожить часть аудита во время атаки или незаконной операции. Выборочное уничтожение аудита является сложной задачей, так что, как правило, разрыв заметен. Вторая особенность атаки, связанной с аудитом, это атака самого сервера времени, так что существует необходимость провести аудит точности сервера времени (было ли сбросов больше, чем обычно?) и аудит клиента для того, чтобы раскрыть возможные инциденты.

Примечание по внедрению. Маршрутизаторы являются хорошим местом (закрытым и подключенным), чтобы служить в качестве серверов времени для того, чтобы гарантировать, что системы синхронизированы. Приложение может/ должно быть готовым обнаружить «ненормальные» пробелы в трафике аудита. «Нормальный» трафик аудита должен определяться на местном уровне.

Так как серверы аудита являются главной мишенью, то как можно проверить аудитом, подвергается ли нападению сервер аудита и что мы должны контролировать, если имеет место какое-либо необычное поведение, и входит ли это в область применения сервиса(ов) аудита.

Примечания

1 Большинство систем используют NTP, который создает записи аудита; они должны сохраняться в хранилище данных аудита и контролироваться.

2 Серверы аудита сами по себе должны быть усилены и защищены.

3 Необходимо рассмотреть возможность сохранения местных копий записей аудита.

Согласованное время является обязательной функциональной возможностью и зависит от сервиса аудита (оно должно использоваться и работать, а не быть просто доступным).

Требование. Хранилище аудита и ассоциированные сервисы должны быть защищены, включая средства управления доступом и средства аудита.

А.9 Случай хакера, создающего ложные записи аудита

Современный злоумышленник подключает ноутбук, который создает ложные записи аудита, чтобы скрыть тот факт, что он отключил систему аудита машины, которая подвергается атаке.

(Некоторые локальные политики могут решить использовать цифровые подписи для того, чтобы обнаружить сокрытие записей аудита.)

А.10 Случай просмотра записей аудита хакером и их злонамеренного использования

Записи аудита могут также быть уязвимыми для анализа трафика или изменений с целью удаления важной информации непосредственно во время передачи.

Смягчение. Не вносить личную медицинскую информацию в записи аудита! Если это невозможно, записи аудита могут быть зашифрованы либо по каждой записи, либо по сессии / потоку.

А.11 Случай странного (уполномоченного/неуполномоченного) изменения конфигурации

Некто, действуя как системный администратор, устанавливает обновление программного обеспечения местной системы. (Альтернатива: вредоносные атаки / случайный злоумышленник устанавливает HTTP-регистратор и фиксирует весь трафик HTTP для обнаружения уязвимостей системы.)

Процесс аудита должен фиксировать дату, время и место обновления, а также «описание изменения», которое включает в себя номера версий программного обеспечения, контрольные суммы файлов и т. д.

Хранилище аудита (или хранилище аудита конфигурации) должно быть время от времени исследовано, чтобы убедиться, что авторизованные обновления конфигурации имели место, когда должны были, и обнаружить несанкционированные или неожиданные изменения конфигурации.

Журнал / сервис аудита также должен записывать все изменения конфигурации, обновления и т. д., в том числе установку программного обеспечения, установку оборудования и изменения конфигурации.

Система аудита должна поддерживать корректирующие действия, а также выполняемый в реальном времени анализ для обнаружения неблагоприятных происходящих событий.

Желательно, что более трудно, распространять это на оборудование.

А.12 Случай пользователя, пытающегося взломать пароль методом грубой силы

Сервер аудита получает отчеты о множестве сбоев при входе в систему и должен быстро установить флаг / запустить сигнал тревоги.

Приложение В
(справочное)

Сервисы журнала аудита

В.1 Сервисы в диаграмме

Диаграмма класса аудита сервисно-ориентированной архитектуры (SOA) на рисунке В.1 служит иллюстрацией сервисов журналов аудита, описанных в настоящем приложении.

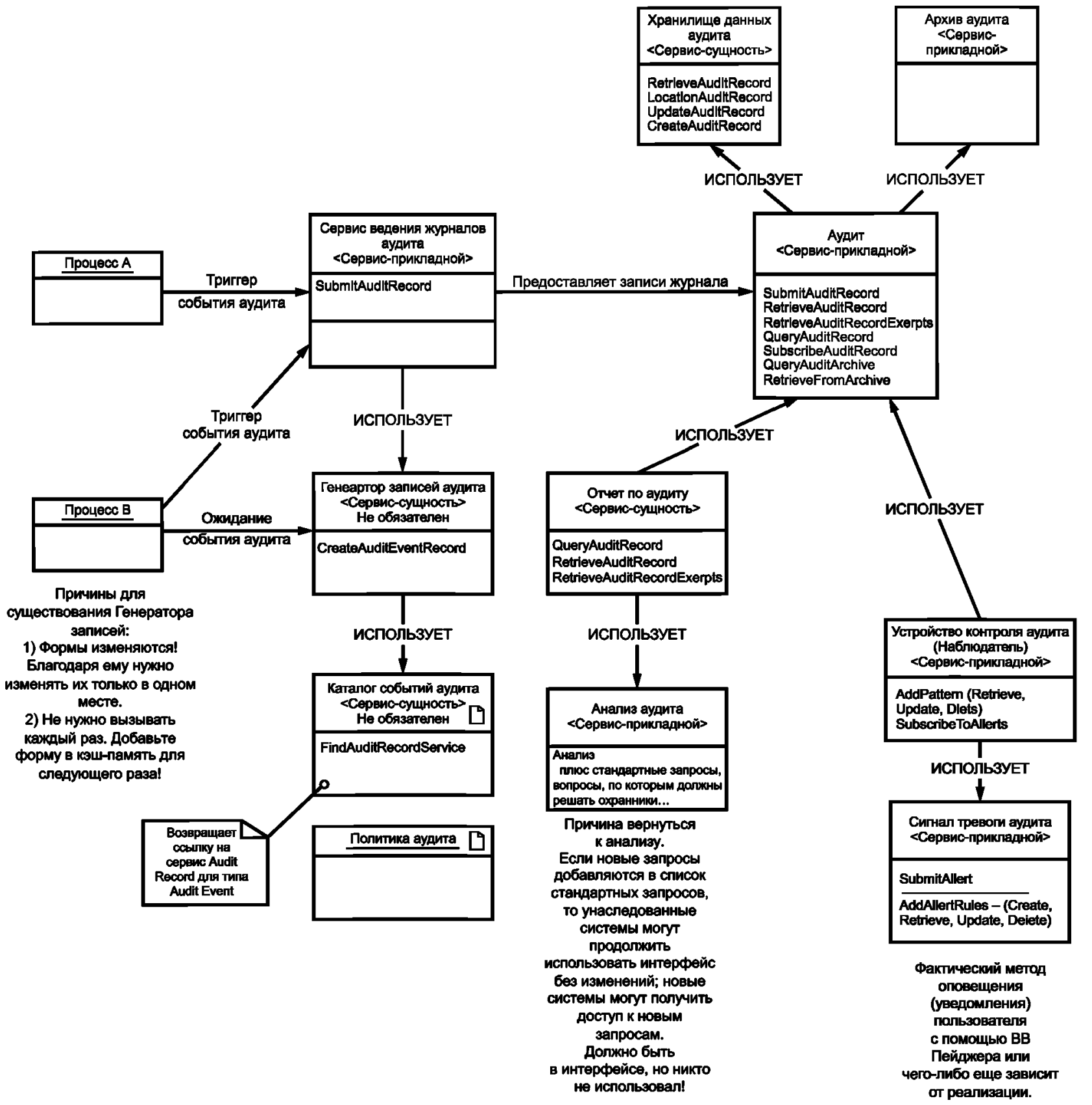


Рисунок В.1 — Диаграмма класса аудита

B.2 Сервис ведения журнала аудита (Audit Logger Service)

Название функциональной возможности — SubmitAuditEvent (Предоставить Событие Аудита).

Описание. Добавляет событие аудита, которое необходимо обработать.

Предварительное условие:

- запись события аудита не является пустым значением;
- запись события аудита соответствует схеме (запись не будет отклонена, если она не соответствует).

Входные данные. Запись события аудита (детали подлежат определению).

Выходные данные. Пустое значение.

Выходные условия. Запись принята.

Условия исключения

Отчет об ошибке, если событие не может быть записано из-за того, что:

- AuditEventRecord является пустым значением;
- AuditEventRecord не соответствует схеме;
- сервис временно недоступен;
- сервис недоступен (основная проблема обеспечения дистанционной связи).

Примечание — Исключения могут быть проигнорированы программой, но должны быть внедрены системой аудита.

Связь с уровнями соответствия

Прочие примечания. Предположения:

- у системы должно быть единое время;
- у хранилища будет функциональная возможность «разветвлять» его по сервисам контроля, пейджерам, всюду, куда должна быть отправлена информация в зависимости от события;
- необходима способность сообщать Audit Event Record Schema (схему записи события аудита);
- для надежных результатов у клиента и систем сервиса должно быть согласованное время.

(У хранилища будет возможность «разветвлять» его по сервисам контроля, пейджерам, всюду, куда должна быть отправлена информация в зависимости от события) — не входит в спецификацию клиента, но это стоит рассмотреть позже.

Другое значимое содержание. При подробном описании необходимо рассмотреть вопросы надежной доставки, кэширования, мониторинга и т. д.

B.3 Сервис генератора записей аудита (Audit Record Generator Service)

Название функциональной возможности — CreateAuditEventRecord (СоздатьЗаписьСобытияАудита) (ДОПОЛНИТЕЛЬНАЯ).

Описание. *Создает фиктивную запись о событии аудита.*

Предварительное условие. *Пустое значение.*

- Входные данные: AuditEventType (ТипСобытияАудита).
- Выходные данные: AuditEventRecord (ЗаписьСобытияАудита).

Постусловия. Создан шаблон фиктивной записи о событии аудита подходящего типа. Если значение AuditEventType — пустое значение, то возвращается фиктивная запись о событии аудита, содержащая все поля каждого типа события (например, применяются все стандарты RFC 3881, ИСО 12052:2006 (DICOM) плюс все, что определено местной политикой в качестве обязательных полей, подлежащих аудиту).

Условия исключительной ситуации. AuditEventType не признан. Если тип события не распознан, то с помощью функциональной возможности будет отправлено в ответ предупреждение, список всех признанных типов событий плюс полная схема всех возможных полей.

Связь с уровнями соответствия. Подлежит определению.

Прочие замечания

Целью этой функциональной возможности является добавление возможности изменения схемы в одном месте и разрешения для всех приложений делать примечания касательно того, что схема изменилась, и обновления схемы, которую они используют без необходимости менять какой-либо код.

С помощью этой функциональной возможности также можно сообщать приложению о том, какая информация требуется для представления события аудита. Она также дает возможность иметь несколько хранилищ, или хранить как локально, так и удаленно без необходимости ставить в известность клиента.

AuditRecordGenerator (ГенераторЗаписейАудита) может использовать AuditEventCatalog (КаталогСобытий Аудита) для того, чтобы определить надлежащие схемы для запрашиваемого типа события. Это, наряду с исключением неточной схемы в AuditLogger (УстройствоВеденияЖурналаАудита), позволит клиентам обнаруживать, когда локальная копия схемы, которую они сохранили в кэш-памяти, устарела и разрешать распространить среди клиентов новые версии схемы без изменения кода.

Другое значимое содержание

Это дополнительный сервис. Опытные разработчики сохранят отклик в кэш-памяти на стороне клиента для экономии времени для схем, которые не изменились.

B.4 Сервис каталога событий аудита (Audit Event Catalog Service)

Название функциональной возможности — FindAuditEventService (НайтиСервисСобытияАудита).

Описание. *Возвращает (ссылку на?) схему события аудита для запрошенного типа. Этот сервис не является непосредственно видимым для клиента, но открыт для использования сервисами ведения журнала аудита и генератора записей аудита.*

Предварительное условие. *Пустое значение.*

- Входные данные: AuditEventType.
- Выходные данные: AuditEventSchema (ссылка?).

Инварианты

Постусловия

- Условия исключительной ситуации. AuditEventType не является общепризнанным типом.

Связь с уровнями соответствия

Прочие примечания

Данный класс предоставляет базу централизованного хранения для определения схемы AuditEvent и должна использоваться в качестве источника локальных копий схемы в системах клиентов. Через AuditRecordGenerator схемы могут быть автоматически распространены среди клиентов.

Другое значимое содержание

Это просто сервис фоновой обработки. Косвенно доступный для клиента через предыдущий сервис.

B.5 Сервис устройства контроля аудита (Audit Monitor Service)

Примечание — Определение сигнала тревоги — это то, что отправляется, когда сервис устройства контроля обнаруживает, что серии событий соответствуют шаблону поведения.

alertName (имя сигнала тревоги) определяется как шаблон событий с уникальным именем, например, «поиск идентификатора данного субъекта данных». В реальной жизни, если есть повод переживать, что кто-то шпионит за субъектом данных, то каждый случай доступа к информации этого субъекта данных должен вызывать сигнал тревоги.

Название функциональной возможности: SubscribeToAlert (ПодписатьсяНаПредупреждение).

Описание. *Вызывается сервисами AuditAlert для уведомления сервиса устройства контроля аудита о том, что сервис AuditAlert хочет получать оповещение в случае сигнала тревоги системы защиты.*

Входное условие — *alertName действительно, т. е. имеет ассоциированный с ним шаблон, который был добавлен.*

Входные данные

- alertName (Примечание — Некоторые имена alertName могут быть предопределены, но в противном случае добавляют только шаблоны);
- subscriberReference (Примечание — В протоколе SOAP это был бы конечный адрес веб-сервиса, в Java — это адрес интерфейса. Ссылка должна быть уникальной во избежание коллизий).

Выходные данные. Пустое значение.

Инварианты

Постусловия

- Сервис AuditAlert, пославший сигнал тревоги, теперь известен для устройства контроля AuditMonitor;
- Условия исключительной ситуации. Недействительное имя alertName.

Прочие примечания

Предположение. Язык шаблонов был всеми согласован.

Для того, чтобы иметь возможность «подписаться, А ТАКЖЕ получить историю событий за последний час», интерфейс может вызывать обе эти функциональные возможности ПЛЮС функциональную возможность queryauditrecords из Сервиса отчетов аудита.

Примечание — Необходимо обозначить, как захватывать и использовать параметр, позволяющий пользователю обозначать дату окончания срока подписки.

Окончание срока подписки. В сервисе устройства контроля дата не указана. Если клиент хочет, чтобы подписка окончилась, внедрение сервиса оповещений/уведомлений может позволить осуществлять планирование подписок. Сервис устройства контроля должен быть легким в эксплуатации.

Название функциональной возможности — UnsubscribeFromAlerts (ОтписатьсяОтПредупреждений).

Описание. *Вызывается сервисами AuditAlert для уведомления сервиса устройства контроля аудита о том, что сервис AuditAlert больше не хочет получать оповещения о событиях аудита.*

Следует отметить, что подписка на сервис устройства контроля — это не то же самое, что и подписка на сервис оповещений. На сервис оповещений подписываются лица в разное время. На сервис устройства контроля подписываются такие сервисы, как сервис оповещений. Это более простой сервис, направленный на сравнение шаблонов, на несложные сигналы тревоги и оповещение.

Предусловие

Входные данные

- alertName;
- subscriberReference (ссылка Подписчика).

Выходные данные. Пустое значение.

Выходные условия: подписка больше не зарегистрирована.

Условия исключения

Связь с уровнями соответствия

Прочие примечания

Другое значимое содержание. Отправить событие аудита!

Название функциональной возможности — AddPattern (ДобавитьШаблон)

Описание. *Позволяет сервису AuditAlert указыватьь новый тип шаблона событий для поиска со спецификацией касательно того, как определять, что наступило условие для отправки сигнала тревоги.*

Предварительное условие

- alertName не является пустым значением и является уникальным;
- eventPattern (шаблон события) не является пустым значением и надлежащим образом обозначено.

Входные данные: alertName, eventPattern.

Выходные данные: пустое значение.

Постусловия. К шаблонам, о которых знает AlertMonitor, добавлен новый шаблон, связанный с именем alertName.

Условия исключения:

- alertName уже существует;
- alertName является пустым значением;
- eventPattern недействителен.

Связь с уровнями соответствия

Прочие примечания

Предположение. Язык шаблонов был всеми согласован.

Предположение. Шаблоны каким-то образом ассоциированы с создателем…

Политика доступа к определенным экземплярам может быть такой: «этот пользователь/ URL/ и т. д. может модифицировать…»

Другое значимое содержание. Отправить событие аудита.

Название функциональной возможности — RetrievePattern (Вернуть Шаблон)

Описание. *Позволяет сервису AuditAlert вернуть шаблон. Если имя alertName недействительно или является пустым значением, то эта функциональная возможность возвращает список всех шаблонов.*

Входное условие

Входные данные: alertName.

Выходные данные: подробные данные о шаблоне или списке всех зарегистрированных или доступных шаблонов.

Постусловия: Шаблон или список шаблонов.

Условия исключения: нет.

Прочие примечания

Это событие само себя проверяет аудитом. Местные политики должны решать, является ли это сервисом, который отправляет событие аудита, или приложением, которое его использует, т. е. это должны определить разработчики.

Другое значимое содержание (дополнительное). Отправить событие аудита.

Название функциональной возможности — DeletePattern (Удалить Шаблон)

Описание. *Удаляет шаблон, который более не применяется. Если все еще есть получатели, подписанные на шаблон, и параметр forcedDelete (принудительноеУдаление) присутствует и является истинным, то Удаление является принудительным Delete. Если параметр НЕ присутствует и все еще есть получатели, подписанные на шаблон, то событие DeletePattern будет неуспешным и запрашивающему лицу будет отправлено исключение.*

Входное условие. alertName не является пустым значением.

Входные данные:

- alertName;
- параметр ForcedDelete.

Выходные данные: пустое значение.

Постусловия

- Шаблон и все подписчики этого шаблона удалены.
- Например, выходные данные — пустое значение.

Условия исключения. Если у предупреждения существуют подписчики и forcedDelete не присутствует и не является истинным, отправить исключение удаленному инициатору запроса.

Связь с уровнями соответствия

Прочие примечания. Удаление подписчиков должно известить инициатора и/или подписчиков.

Не забудьте «запустить событие» о том, что подписчики все еще есть. Другая деятельность по обращению или перечислению подписчиков может быть оставлена на этап реализации.

Если это доступно, DeletePattern должен посылать список остающихся подписчиков при неудаче удаления.

Другое значимое содержание. Отправить событие аудита.

B.6 Сервис сигнала тревоги или оповещения (Alert or Notification Service)

Название функциональной возможности — SubmitNotification (НаправитьУведомление).

Описание. *Направляет сообщение с сигналом тревоги, которое должно быть обработано.*

Предусловие

Входные данные: NotificationMessage (СообщениеУведомления).

Выходные данные: пустое значение.

Выходные условия. AlertMessage отправлено в соответствии с применимыми правилами.

Условия исключения:

- AlertMessage является пустым значением;
- ошибка обработки AlertMessage.

Связь с уровнями соответствия

Прочие примечания

Реальный метод для оповещения пользователя (например, пейджер или другое средство) является зависимым от реализации.

Другое значимое содержание. Отправить событие аудита после направления сигнала тревоги.

Название функциональной возможности — SetNotificationRuleSet (УстановитьНаборПравилОповещения).

Описание. *Создает и поддерживает соответствие правилам, используемым для определения того, как необходимо обрабатывать AlertMessage.*

Предусловие. AlertRuleSet (НаборПравилСигналаТревоги) не является пустым значением.

Формат AlertRuleSet должен быть признанным и обрабатываемым Сервисом.

Входные данные: AlertRuleSet.

Выходные данные: пустое значение.

Предусловия. Был установлен новый AlertRuleSet.

Условия исключения:

- AlertRule является пустым значением;
- неизвестное правило.

Связь с уровнями соответствия

Название функциональной возможности — RetrieveAlertRules (ВернутьПравилаСигналаТревоги).

Описание. *Возвращает копию правил для сигналов тревоги, действующих в данном сервисе.*

Предусловие. Нет.

Входные данные: нет.

Выходные данные: AlertRules.

Инварианты. AlertRules не изменены.

Постусловия. Выход AlertRules содержит полный набор действующих AlertRules.

Условия исключения. Нет.

Связь с уровнями соответствия

Прочие примечания

Другое значимое содержание

B.7 Сервис отчетов аудита (Audit Report Service)

Название функциональной возможности — QueryAuditService (СервисАудитовОпроса).

Описание. *Опрашивает Сервис аудита для записей, соответствующих шаблону или параметрам опроса, запрошенным в фильтре опроса.*

Предусловие. *QueryFilter (ФильтрЗапроса) не является пустым значением. Если запрашиваются все записи, то должен использоваться шаблон * (или его эквивалент в оговоренном языке запросов).*

Язык фильтра запроса должен быть оговорен.

Входные данные: QueryFilter.

Выходные данные: список уникальных идентификаторов для запрошенных записей.

Постусловия. Идентификаторы записей, соответствующие фильтру запроса, были получены.

Условия исключения:

- QueryFilter является пустым значением;
- QueryFilter не может быть проанализирован.

Связь с уровнями соответствия

Прочие примечания

Другое значимое содержание

Название функциональной возможности — RetrieveAuditRecord (ВернутьЗаписьАудита).

Описание. *Возвращает определенную запись аудита.*

Предусловие. *RecordId (ИдентификаторЗаписи) не является пустым значением.*

Входные данные: RecordId.

Выходные данные: запрашиваемая запись, если таковая существует. В противном случае — пустое значение.

Постусловия. Запись, соответствующая RecordId, получена.

Условия исключения. RecordId является пустым значением.

Название функциональной возможности — RetrieveAuditRecordExcerpt (ВернутьОтрывокЗаписиАудита)

Описание. *Возвращает отрывок, определенный описаниями полей из записи, подходящей по идентификатору записи.*

Предусловие. *Идентификатор записи не является пустым значением.*

Описания полей действительны.

Входные данные:

- RecordId;
- FieldDescriptions (ОписанияПолей).

Выходные данные: отрывок записи аудита, соответствующий полям запроса из записи, подходящей по идентификатору, если такой идентификатор существует. В противном случае — пустое значение.

Постусловия. Запрашиваемый отрывок получен.

Условия исключения:

- RecordId является пустым значением;
- FieldDescriptions недействительны.

Связь с уровнями соответствия

B.8 Сервис анализа аудита (Audit Analysis Service)

Название функциональной возможности — Analyze (Анализировать).

Описание. *Осуществляет запрошенный анализ.*

Предусловие. *Запрос анализа является действующим алгоритмом.*

Входные данные: AnalysisAlgorithm (АлгоритмАнализа).

Выходные данные: AnalysisReport (ОтчетПоРезультатамАнализа).

Постусловия. AnalysisAlgorithm был выполнен и результаты получены.

Условия исключения. AnalysisAlgorithm недействителен.

Связь с уровнями соответствия.

Приложение ДА
(справочное)

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

Таблица ДА.1

Обозначение ссылочного международного стандарта, документа	Степень соответствия	Обозначение и наименование соответствующего национального стандарта
ИСО 8601:2004	—	*
ИСО 27799:2008	—	*

* 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.

Библиография

[1] ISO 12052:2006, Health informatics — Digital imaging and communication in medicine (DICOM) including workflow and data management

[2] ISO/TS 14265:2011, Health Informatics — Classification of purposes for processing personal health information

[3] ISO 15489-1:2001, Information and documentation — Records management — Part 1: General

[4] ISO/TS 21298:2008, Health informatics — Functional and structural roles

[5] ISO/TS 21547:2010, Health informatics — Security requirements for archiving of electronic health records — Principles

[6] ISO/TS 22600 (all parts), Health informatics — Privilege management and access control

[7] ISO/IEC 8824-1, Information technology — Abstract Syntax Notation One (ASN.1): Specification of basic notation — Part 1

[8] ISO/IEC 8824-2, Information technology — Abstract Syntax Notation One (ASN.1): Information object specification — Part 2

[9] ISO/IEC 15408-2:2008, Information technology — Security techniques — Evaluation criteria for IT security — Part 2: Security functional components

[10] ASTM E2147-01, Standard Specification for Audit and Disclosure Logs for Use in Health Information Systems

[11] DICOM. Supplement 95: Audit Trail Messages, Final Text 27 August 2010, now incorporated in DICOM Part 15: http://medical.nema.org/standard.html

[12] IHE IT Infrasructure Technical Framework, Volume 1: Integration Profiles and Volume 2: Transactions

[13] IETF RFC 3881:2004, Security Audit & Access Accountability Message — XML Data Definitions for Healthcare Applications

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

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

[16] ISO/IEC 27000:2012, Information technology — Security techniques — Information security management systems — Overview and vocabulary

[17] ASTM E1769:1995, Standard Guide for Properties of Electronic Health Records and Record Systems

[18] IEC 60050-713:1998, International Electrotechnical Vocabulary — Part 713: Radiocommunications: transmitters, receivers, networks and operation

[19] IETF RFC 4810, Long-Term Archive Service Requirements

[20] IETF RFC 4998, Evidence Record Syntax (ERS)

УДК 004:61:006.354 ОКС 35.240.80 П85 ОКСТУ 4002

Ключевые слова: здравоохранение, информатизация здоровья, структуры данных, электронные медицинские карты, регистрационный журнал

Редактор *А.Ф. Колчин*
Технический редактор *В.Ю. Фотиева*
Корректор *М.В. Бучная*
Компьютерная верстка *Е.А. Кондрашовой*

Сдано в набор 13.07.2016. Подписано в печать 27.07.2016. Формат 60×84⅛. Гарнитура Ариал.
Усл. печ. л. 5,12. Уч.-изд. л. 4,67. Тираж 28 экз. Зак. 1787.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

Издано и отпечатано ФГУП «СТАНДАРТИНФОРМ», 123995 Москва, Гранатный пер., 4.
gost.e-ecolog.ru gost.e-ecolog.ru

gost.e-ecolog.ru