ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р ИСО/ТС 22600-1— 2009

Информатизация здоровья

УПРАВЛЕНИЕ ПОЛНОМОЧИЯМИ И КОНТРОЛЬ ДОСТУПА

Часть 1

Общие сведения и управление политикой

ISO/TS 22600-1:2006
Health informatics — Privilege management and access control — Part 1: Overview and policy management
(IDT)

Издание официальное

БЗ 8—2009/430

Москва
Стандартинформ
2010

gost.e-ecolog.ru

Предисловие

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

Сведения о стандарте

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

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

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 14 сентября 2009 г. № 410-ст

4 Настоящий стандарт идентичен международному стандарту ИСО/ТС 22600-1:2006 «Информатизация здоровья. Управление полномочиями и контроль доступа. Часть 1. Общие сведения и управление политикой» (ISO/TS 22600-1:2006 «Health informatics — Privilege management and access control — Part 1: Overview and policy management»)

5 ВВЕДЕН ВПЕРВЫЕ

Информация об изменениях к настоящему стандарту публикуется в ежегодно издаваемом информационном указателе «Национальные стандарты», а текст изменений и поправок — в ежемесячно издаваемых информационных указателях «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ежемесячно издаваемом информационном указателе «Национальные стандарты». Соответствующая информация, уведомление и тексты размещаются также в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет

© Стандартинформ, 2010

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

Содержание

1 Область применения . . . 1
2 Термины и определения . . . 2
3 Цели иструктура управления полномочиями и контроля доступа . . . 3
3.1 Цели управления полномочиями и контроля доступа . . . 3
3.2 Структура управления полномочиями и контроля доступа . . . 3
4 Соглашение о политике . . . 6
4.1 Обзор . . . 6
4.2 Идентификация . . . 7
4.3 Информированное согласие пациента . . . 7
4.4 Защита персональных данных пациента . . . 7
4.5 Идентификация информации . . . 7
4.6 Локализация информации . . . 7
4.7 Целостность данных . . . 7
4.8 Безопасность . . . 7
4.9 Авторизация . . . 7
4.10 Структура ролей . . . 7
4.11 Права аттестации . . . 8
4.12 Делегирование прав . . . 8
4.13 Срок действия . . . 8
4.14 Аутентификация пользователей и ролей . . . 8
4.15 Доступ . . . 8
4.16 Срок действия соглашения . . . 8
4.17 Этические принципы . . . 8
4.18 Защищенный регистрационный журнал . . . 8
4.19 Аудиторская проверка . . . 8
4.20 Анализ рисков . . . 8
4.21 Непрерывность и управление чрезвычайными ситуациями . . . 8
4.22 Развитие информационных систем . . . 9
5 Документация . . . 9
Приложение А (справочное) Пример шаблона документации . . . 10
Приложение В (справочное) Пример соглашения о политике обмена информацией . . . 16
Библиография . . . 20

Введение

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

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

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

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

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

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

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

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

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

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

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

Применение настоящего стандарта будет вызывать особую сложность в связи с тем, что участвующие стороны уже располагают действующими системами и не проявят особого желания немедленно обновить их или полностью заменить. Поэтому очень важно, чтобы стороны подписали соглашение о

политике, в котором они подтверждают намерение к движению в сторону реализации настоящего стандарта по мере возникновения потребности в модификации этих систем.

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

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

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

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

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

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

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

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

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

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Информатизация здоровья

УПРАВЛЕНИЕ ПОЛНОМОЧИЯМИ И КОНТРОЛЬ ДОСТУПА

Часть 1

Общие сведения и управление политикой

Health informatics. Privilege management and access control.
Part 1. Overview and policy management

Дата введения — 2010—07—01

1 Область применения

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

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

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

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

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

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

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

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

Издание официальное

2 Термины и определения

В настоящем стандарте применены следующие термины с соответствующими определениями:

2.1 **контроль доступа** (access control): Средства обеспечения доступа к ресурсам системы обработки данных только авторизованным субъектам авторизованными способами [5].

2.2 **отслеживаемость** (accountability): Свойство, обеспечивающее однозначную привязку действий субъекта к конкретному субъекту [6].

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

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

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

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

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

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

2.7 **доступность** (availability): Свойство быть доступным и годным к использованию по запросу авторизованного субъекта [6].

2.8 **уполномоченное лицо по сертификации**; УС (certification authority; CA): Уполномоченное лицо, которому одна или несколько участвующих сторон доверили выпуск и присвоение сертификатов [7].

Примечания

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

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

2.9 **конфиденциальность** (confidentiality): Свойство, заключающееся в том, что информация не может быть доступной или раскрытой для неавторизованных лиц, объектов или процессов [6].

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

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

2.12 **ключ** (key): Последовательность символов, управляющая операциями шифрования и дешифровки [6].

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

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

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

2.16 **секретный ключ** (private key): Ключ, используемый в асимметричном криптографическом алгоритме, обладание которым ограничено (обычно только одним субъектом) [9].

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

2.18 **открытый ключ** (public key): Ключ, используемый в асимметричном криптографическом алгоритме, который может быть сделан общедоступным [9].

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

2.20 **безопасность** (security): Сочетание доступности, конфиденциальности, целостности и отслеживаемости [12].

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

2.22 **сервис безопасности** (security service): Сервис, предоставляемый уровнем взаимодействия открытых систем, обеспечивающий надлежащую степень безопасности систем или передачи данных [6].

2.23 **надежная аутентификация** (strong authentication): Аутентификация, осуществляемая посредством свидетельств, полученных с использованием криптографических средств.

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

3 Цели и структура управления полномочиями и контроля доступа

3.1 Цели управления полномочиями и контроля доступа

Целями управления полномочиями и контроля доступа являются:

a) создание инструкций по совместному использованию информации, включая шаблон соглашения о политике, который задает и определяет структуру и содержание этого документа;

b) создание стандарта управления полномочиями и контроля доступа, который обусловливает безопасный обмен информацией между зонами безопасности. Для этого определен базовый процесс обмена информацией. Стандарт по управлению полномочиями и контролю доступа также определяет метод организации защищенного трансграничного процесса обмена информацией;

c) установление курса на преобразование существующих систем в будущие системы, удовлетворяющие всем критериям трансграничного обмена информацией в соответствии с настоящим стандартом.

Организацию процесса обмена информацией о полномочиях и контроле доступа следует осуществлять с учетом текущей ситуации и предусматривать стандартизацию обмена информацией между зонами безопасности существующих систем. Соглашение о политике, репозиторий политик и каталог являются центральными элементами настоящего стандарта.

3.2 Структура управления полномочиями и контроля доступа

3.2.1 Элементы структуры

Структура модели процесса обмена данными между зонами безопасности состоит из элементов, перечисленных ниже. В настоящем стандарте понятие структуры раскрывается в широком смысле.

Структура состоит из следующих элементов:

- зона;
- политика;
- роли;
- каталог;
- аутентификация;
- процесс.

Правила для этих элементов, согласованные участвующими зонами, хранятся в репозитории и могут рассматриваться как часть данной структуры.

3.2.2 Зона

Чтобы информационная система, обеспечивающая совместный доступ к медицинским данным, была управляемой и работоспособной, ее компоненты, непосредственно связанные с принципалами, группируются в зоны по принципу общности организационных, логических и технических свойств. Функциональная совместимость любого вида в пределах зоны называется внутризональным обменом информацией и взаимодействием, а функциональная совместимость между зонами называется межзональным обменом информацией и взаимодействием. Например, обмен информацией может осуществляться между отделениями больницы в пределах больничной зоны (внутризональный обмен информацией) или быть внешним по отношению к зоне специализированного отделения (межзональный обмен информацией).

Зона может состоять из субзон (которые будут наследовать и могут специализировать политики родительской зоны). Наименьшей зоной может быть отдельное рабочее место или конкретный компонент информационной системы. Зоны могут объединяться в суперзоны связыванием отдельных зон и формированием общей зоны большего масштаба для обмена информацией и взаимодействия.

3.2.3 Политика

3.2.3.1 Политика контроля доступа

Политика описывает концепцию, включая нормы и правила, организационные и административные рамки, функциональности, требования и цели, участвующие стороны, соглашения, заданные права, обязанности и штрафные санкции, а также технические решения, реализованные для сбора, записи, обработки и передачи данных в информационных системах.

Для описания политик могут использоваться такие средства, как шаблоны или формальные модели политик. Модель политики описана в подразделе 4.4 ИСО/ТС 22600-2. Что касается требований по безопасности, то особый интерес представляет политика информационной безопасности. Политика информационной безопасности рассматривается в подразделе 4.1 ИСО/ТС 22600-2.

Политика, рассматриваемая в настоящем стандарте, касается инфраструктуры контроля доступа. Она определяет требования и условия надежного обмена информацией, создания, хранения, обработки и использования важной информации, включает юридические и этические последствия, организационные и функциональные аспекты, а также технические решения.

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

Соглашение о политике представлено в разделе 6 и формально промоделировано с использованием структурных схем и шаблонов в части 2 ИСО/ТС 22600. Процесс выработки соглашения по информационному обмену должен предшествовать процессу реального обмена информацией. Ниже описан сценарий процесса выработки соглашения, которое будет служить основой для процесса реального обмена информацией, описанного в 3.2.7.

3.2.3.2 Процесс выработки соглашения

Процесс выработки соглашения начинается с формирования группы должностных лиц, хорошо осведомленных о системах, участвующих в процессе обмена информацией, и уполномоченных принимать решения о том, какой информацией можно обмениваться и какого уровня защиты она требует.

После принятия решения о том, какой информацией можно обмениваться, надо провести анализ уровня защиты в обеих системах и определить уровень, удовлетворяющий обе стороны. Для этого надо составить список всех требований с обеих сторон и для их оценки составить форму, подобную приведенной в приложении А.

На следующем этапе процесса выработки соглашения стороны сравнивают свои системы по критериям оценки, заполняя оценочную форму. В дальнейшем эти формы составят основу для соглашения сторон об обмене информацией. В каждом случае, когда выявлено несоответствие одной из систем согласованному уровню защиты, этот факт должен быть отмечен в соглашении вместе с описанием необходимых действий. Например, одна из сторон решает, что обмен информацией может быть начат только после устранения данного несоответствия или обмен информацией может быть начат, но данное несоответствие должно быть устранено в указанные сроки.

Участвующие стороны должны также определить и зафиксировать в соглашении сервисы и уровень сервисов репозитория политик. Одним из примеров может служить взаимное отображение ролей, используемых в двух зонах, если они не согласованы.

В соглашении должны быть указаны средства обеспечения управления и функционирования общего каталога и сервисы репозитория политик.

3.2.4 Роли

Право назначения ролей, полномочий и свидетельств, а также принятия окончательного решения о доступе к ресурсу должно быть закреплено за конкретным принципалом. Следовательно, идентификация и аутентификация принципалов являются базовыми сервисами для авторизации, контроля доступа и других сервисов обеспечения безопасности приложений.

Назначение ролей может существенно варьироваться в разных учреждениях здравоохранения как по степени детализации, так и по иерархической организации. Это создает трудности для функциональной совместимости, которые должны быть преодолены при согласовании политик.

Обобщенная концепция ролей описана в 4.4 и в приложении А ИСО/ТС 22600-2, а также будет рассмотрена в разрабатываемом стандарте ИСО/ТС 21298.

3.2.5 Репозиторий политик

Репозиторий политик содержит набор правил контроля доступа и набор ролей, к которым они применяются. Для обеспечения межзонального контроля доступа эти правила и механизм отображения ролей следует хранить в общем репозитории политик.

Общий репозиторий политик является формальным представлением соглашения о политике. Он используется службой контроля доступа вместе с информацией о ролях отдельного субъекта для принятия решения о предоставлении или отказе в доступе. Если все требования выполнены, пользователь приложения из одной зоны безопасности получит полномочие на доступ и получение надлежащей информации из другой зоны безопасности.

3.2.6 Каталог

Служба каталога предоставляет информацию о субъектах. Спецификация каталога должна соответствовать требованиям, изложенным в [14].

Служба общего каталога, используемая для межзонального контроля доступа, должна предоставлять необходимую информацию обо всех субъектах, на которых распространяется соглашение о политике, включая информацию о назначении ролей и аутентификации.

3.2.7 Аутентификация

Существуют различные уровни аутентификации принципалов. Вследствие щепетильности медицинской информации и связанных с этим требований по ее защите при обмене информацией и взаимодействии должен быть обеспечен наивысший уровень защиты как для запрашивающего, так и для отвечающего принципалов посредством надежной взаимной аутентификации. Надежная аутентификация должна быть реализована по технологии, основанной на передаче маркеров (например, с использованием смарт-карт).

Основы аутентификации определены в [8] и [9]. Процедура аутентификации основана на использовании инфраструктуры открытых ключей. Основы инфраструктуры открытых ключей определены в [10]. Сертификат аутентификации соответствует спецификации X.509V3.

3.2.8 Процесс

Лечебно-диагностические процессы подвержены изменениям. Поэтому очень важно создавать решения, позволяющие вносить необходимые изменения в процессы обмена информацией, не затрагивая лечебно-диагностический процесс. Большинство рутинных процедур по назначению и отзыву ролей, а также по авторизации должны быть максимально автоматизированы без потери контроля над информационной безопасностью. В отдельных случаях специалисты, участвующие в лечении пациента, должны иметь возможность выходить за рамки ограничений авторизации, назначенной их ролям, и быть готовыми обосновать это позже.

Содержание процесса различно в разных случаях, но описанный ниже процесс является ведущим процессом для настоящего стандарта. В этом процессе участвуют две зоны безопасности, в каждой из которых функционирует одно приложение.

Сценарием примера является ситуация, когда специалисту из зоны безопасности 1 нужна информация о своем пациенте, хранящаяся в зоне 2, где данный пациент проходил лечение ранее.

В определенных обстоятельствах одному приложению необходимо передать информацию другому приложению и/или получить информацию от него. Эта необходимость определяется пользователями данных приложений. Пользовательский доступ контролируется каждой зоной безопасности, но он может быть также предоставлен по запросу пользователя из другой зоны безопасности. Внешний запрос на доступ удовлетворяется после его успешной проверки на соответствие согласованным правилам, хранящимся в репозитории политик. Все такие правила должны быть указаны в соглашении о политике.

В обеих зонах имеются свои системы авторизации со своими перечнями ролей, соответствующими их потребностям, и разными правилами предоставления доступа к разной информации для разных ролей.

Модель процесса представлена на рисунке 1.

Процесс осуществляется в следующей последовательности:

1) Новый сотрудник получает свою роль, определенную и назначенную руководителем подразделения, в котором он собирается работать, в соответствии с изложенным в 3.2.4.

2) Новый сотрудник регистрируется в системе авторизации соответствующей зоны безопасности с ограничениями и авторизацией, присущими назначенной ему роли. Это подразумевает, что сотрудник аутентифицируется в соответствии с изложенным в 3.2.7.

3) Пользователи из двух зон безопасности, которые удовлетворяют правилам, определенным в соглашении о политике, могут быть найдены через службу общего каталога. Каталог доступен из любого приложения в зонах безопасности, на которые распространяется соглашение о политике. См. 3.2.6.

4) Когда сотрудник, принадлежащий к зоне безопасности 1, начинает использовать приложение 1 в информационной системе 1 зоны безопасности 1, первым, что должно сделать данное приложение, является проверка его авторизации в службе контроля доступа 1 (см. рисунок 1).

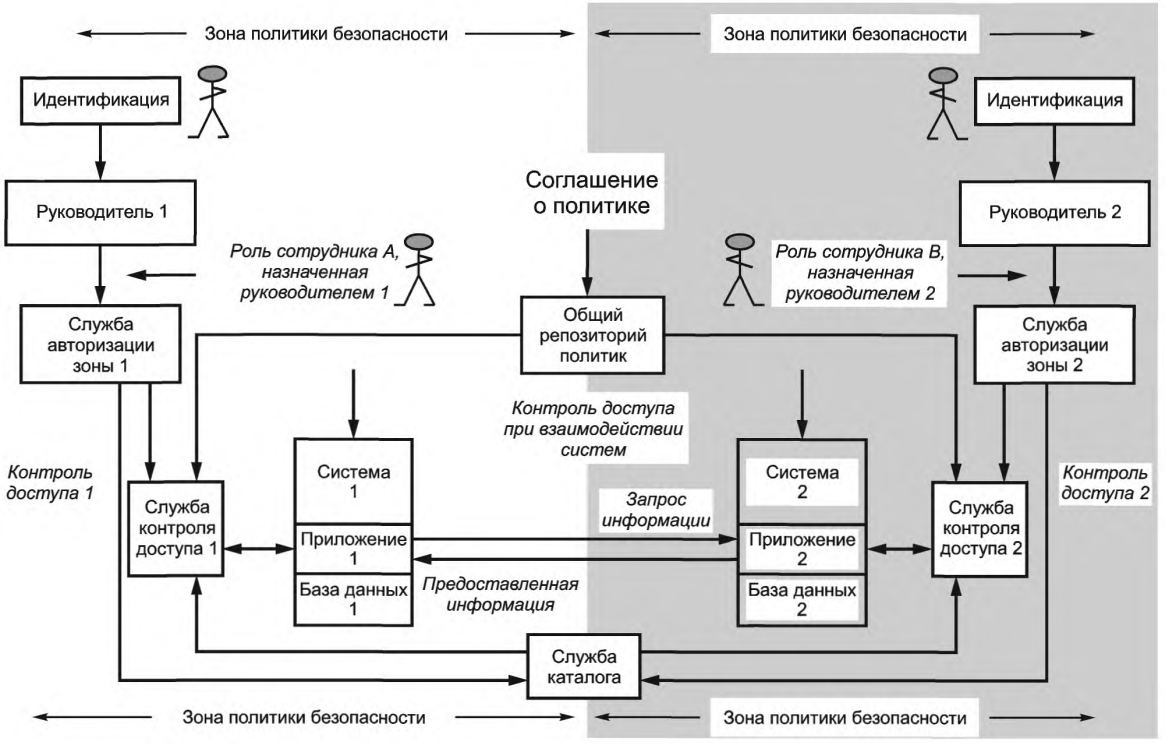

Рисунок 1 — Модель процесса

5) Сотруднику предоставляется доступ к приложению 1 в зоне безопасности 1. Правила внутризонального и межзонального информационного взаимодействия описаны в подразделе 4.1 ИСО/ТС 22600-2.

6) Сотрудник, использующий приложение 1, создает запрос на получение информации от приложения 2 из зоны безопасности 2. Запрос содержит идентификацию и роль запрашивающего, а также ссылку на соответствующее правило в общем репозитории политик.

7) В этой ситуации обе системы обратятся к репозиторию политик, чтобы проверить, выполняются ли требования к обмену информацией. Поэтому необходимо, чтобы для зон 1 и 2 была согласована политика для данного типа обмена информацией, и чтобы в репозитории политик имелись правила для проверки допустимости данного обмена. Если все эти условия выполнены, то процесс продолжается с шага 8. В противном случае приложение 1 должно уведомить пользователя, что его запрос отклонен.

8) Приложение 1 посылает запрос на получение информации приложению 2 из зоны безопасности 2.

9) Результат запроса посылается приложению 1, в котором сотрудник может его прочитать и сохранить вместе с другой информацией о данном пациенте.

10) Все транзакции, имевшие место в приложении 1, приложении 2, службе каталога и репозитории политик, а также все взаимодействия между двумя зонами должны регистрироваться. Стандартные процедуры мониторинга журнала регистрации должны быть определены в соглашении о политике.

4 Соглашение о политике

4.1 Обзор

Основная часть соглашения о политике должна содержать описание действующей юридической базы, включая правила и нормы. В нем должны быть прописаны организационные и административные решения, функциональность, требования и цели, участвующие принципалы, соглашения, права, обязанности и наказания, а также технические решения, применяемые для сбора, записи, обработки и передачи данных в приложениях в зонах безопасности.

Соглашение о политике должно также содержать стандартизированный документ, целью которого является облегчение написания соглашения, покрывающего функции, необходимые для обмена информацией. Стандартный шаблон соглашения о политике представлен в приложении А.

Следует также принять меры, гарантирующие однозначное понимание соглашения о политике каждым лицом, пользующимся межзональным обменом информацией. Ответственность за соблюдение соглашения лежит на главных администраторах зон безопасности.

Функции описаны в 4.2—4.22.

4.2 Идентификация

Соглашение о политике должно определять методы идентификации, используемые в зонах безопасности, включая идентификацию лиц (пациентов, медицинских специалистов, других работников здравоохранения и т. д.), организаций, систем, устройств, приложений, компонентов и т. д. При использовании разных систем идентификации каждая из них должна быть определена. Также должны быть определены механизмы связывания, отображения и преобразования. В данном контексте необходимо рассмотреть и задать использование уникального идентификатора пациента, а также главного регистра пациентов, связанного с пространством имен, и служб идентификации пациентов.

4.3 Информированное согласие пациента

Правила получения и хранения информированного согласия пациента должны быть согласованы, в противном случае должны быть установлены пути преодоления разногласий. Принятое решение должно быть зафиксировано в соглашении о политике.

4.4 Защита персональных данных пациента

Защита персональных данных пациента является ключевым вопросом при трансграничном обмене информацией.

Чтобы добиться полного доверия пациента к информационным транзакциям, крайне важно, чтобы правила были ясны и пациенты легко их понимали.

4.5 Идентификация информации

Соглашение о политике должно идентифицировать процедуру доступа к данным, хранящимся в другой зоне безопасности. Поскольку существует много способов обеспечения такого доступа, очень важно, чтобы выбранный способ был описан в соглашении.

Если данные предназначены только для чтения, то внешний пользователь может получить такие же права доступа к приложению в другой зоне безопасности, что и обычный пользователь этой зоны. Если же внешний пользователь хочет передать информацию в другую зону безопасности, то должна быть предусмотрена возможность указать или идентифицировать и ограничить информацию, подлежащую передаче.

4.6 Локализация информации

Чтобы обеспечить защиту передаваемой информации, необходимо определить структуры данных, используемые в приложениях, в понятной для всех сторон форме. Поэтому соглашение о политике должно содержать подробные описания передаваемой информации и структуры данных.

4.7 Целостность данных

Для выявления искажения данных в процессе передачи между зонами безопасности должна выполняться проверка целостности данных. Правила и методы такой проверки должны быть согласованы и зафиксированы в соглашении о политике.

4.8 Безопасность

С большой вероятностью каждая зона будет иметь свои собственные правила безопасности. Конечно, было бы идеально, если бы все участвующие зоны могли перейти к единой модели безопасности. Это является основной целью, и стандарты информационной безопасности, принятые Европейским комитетом по стандартизации и ИСО, должны служить главными инструментами ее достижения.

Если такой переход невозможен, то в соглашении должно быть определено, какой уровень защищенности в одной зоне соответствует какому уровню защищенности в другой зоне. Также должны быть разработаны полномочия пользователей для разных уровней защищенности в обеих зонах.

Примечание — Аспекты информационной безопасности рассматриваются в ИСО/ТС 22600-2.

4.9 Авторизация

В соглашении о политике должны быть определены процессы авторизации как внутренний, в пределах зоны безопасности, так и внешний, относящийся к другим зонам безопасности. Более подробно авторизация рассмотрена в разделе 4 ИСО/ТС 22600-2.

4.10 Структура ролей

Роли определяются для каждой зоны. В политиках определяются права и обязанности для одной или нескольких ролей в конкретных контекстах. Назначение ролей является очень важной частью при

разработке окончательного стандарта по согласованию политик. Модель ролей представлена в подразделах 4.6—4.9 ИСО/ТС 22600-2.

4.11 Права аттестации

В соглашении о политике должны быть перечислены лица, имеющие право назначать роли и засвидетельствованные полномочия сотрудникам организации. Уполномоченный сотрудник имеет право категорировать медицинскую информацию.

4.12 Делегирование прав

В повседневной работе нередко возникает потребность в делегировании прав. Для управления этим процессом делегирование прав должно быть определено в соглашении, так как крайне трудно точно знать, кто наделен какими правами внутри своей зоны безопасности и в других зонах. Делегирование должно быть хорошо структурированным, чтобы его можно было отслеживать. Модель делегирования рассматривается в подразделе 4.8 ИСО/ТС 22600-2.

4.13 Срок действия

Авторизация, роли, права аттестации и делегирование прав должны иметь четко определенные сроки действия по отношению к правам доступа к информации как внутри своей зоны безопасности, так и в других зонах. Эти сроки должны быть указаны в соглашении.

4.14 Аутентификация пользователей и ролей

В качестве метода аутентификации рекомендуется использовать инфраструктуру открытых ключей. В настоящем стандарте определен ряд условий, которые должны быть выполнены, если между зонами безопасности не может быть достигнуто соглашение о единой стандартизованной системе аутентификации.

4.15 Доступ

Обстоятельства, при которых разрешается доступ к информации в другой зоне безопасности, описаны в подразделе 4.7 ИСО/ТС 22600-2.

Правила для прав доступа должны быть согласованы и установлены в соглашении.

4.16 Срок действия соглашения

В соглашении должен быть установлен срок его действия. Соглашение должно также содержать пункт, определяющий процедуру прекращения действия соглашения как по окончании срока его действия, так и досрочно. Должны быть определены законные основания для расторжения соглашения. В соглашении также должны быть определены штрафные санкции в случае его досрочного расторжения.

4.17 Этические принципы

Нормы и правила никогда не охватывают все возможные ситуации. Поэтому должны учитываться этические принципы, и должен быть сформулирован меморандум, позволяющий каждому получить четкое понимание рамок своей ответственности, в которых он должен действовать.

4.18 Защищенный регистрационный журнал

Как было указано выше, все транзакции должны регистрироваться в журнале. В соглашении должно быть указано, как это будет делаться и с какой степенью детализации. Регистрация транзакций является ключевым фактором доверия пациентов к системе.

Чтобы гарантировать высокое качество ведения регистрационного журнала, необходимо использовать метки времени. Все информационные транзакции должны иметь метку времени. Это может потребовать существенного перепрограммирования более старых систем и, следовательно, может оказаться невозможным по экономическим причинам. В этом случае стороны, подписывающие соглашение, должны решить, что можно сделать в существующих обстоятельствах и какие меры должны быть приняты для исправления ситуации. План реализации этих мер является частью соглашения.

4.19 Аудиторская проверка

В соглашении должно быть оговорено, когда, кем и каким образом должны проверяться файлы регистрационного журнала и предприниматься надлежащие действия.

4.20 Анализ рисков

При наличии каких-либо рисков все стороны должны совместно оценить их и решить, приемлемы они или нет. Риски должны быть задокументированы в соглашении о политике. Если риски приемлемы, то все стороны должны одобрить соглашение о политике. Если риски не приемлемы, то в соглашение о политике должен быть включен план, детализирующий требования к ресурсам, обеспечивающим снижение рисков.

4.21 Непрерывность и управление чрезвычайными ситуациями

В соглашении о политике должны быть определены подробные процедуры для поддержания непрерывности бизнес-процессов, восстановления работоспособности и управления чрезвычайными ситуациями в случае сбоев.

4.22 Развитие информационных систем

Для обеспечения не только текущего, но и будущего обмена данными между информационными системами все стороны должны принять на себя в соглашении о политике обязательство развивать свои информационные системы в соответствии с настоящим стандартом и другими принятыми стандартами.

Все эти функции должны быть определены в соглашении о политике. Стандартизированный формат соглашения о политике описан в приложении В и должен использоваться в качестве руководства при составлении соглашения о политике.

В соглашении о политике должны быть определены все функции обмена информацией.

5 Документация

Соглашение о политике основывается на документации по информационной безопасности систем, участвующих в информационном обмене. Все стороны должны документировать информационную безопасность своих систем в стандартизированной форме, чтобы ее можно было сопоставить. Документация состоит из двух частей.

Первая часть, являющаяся административной, определяет системы, участвующие в информационном обмене, и ответственных лиц. В ней также указывается версия документации, дата и время выпуска и внесения изменений.

Вторая часть, упорядочивающая документацию системы, состоит из ряда вопросов относительно систем, участвующих в информационном обмене. Каждый вопрос разделен на две части. Первая часть касается текущей ситуации, а во второй части спрашивается, что предполагается предпринять, чтобы выполнить требования по обеспечению информационной безопасности. На каждый вопрос в документации предлагается список ответов, ранжирующихся от полного выполнения требований до их невыполнения. Лицо, заполняющее документ, может выбрать ответ, в наибольшей мере подходящий для данного вопроса. Крайне важно, чтобы списки стандартизованных ответов с множественным выбором были четко определены и понятны для обеих сторон.

Любое различие в ответах на вопросы «как есть сейчас?» и «как должно быть?» является фактором риска для информационной безопасности. Должен быть проведен анализ того, какие риски могут вытекать из выявленных различий. Необходимо задокументировать эти риски и описать меры по их устранению.

Пример шаблона стандартной документации приведен в приложении А.

Приложение А
(справочное)

Пример шаблона документации

А.1 Введение

Стороны, совместно использующие информацию, должны общими усилиями создать единый шаблон документации, охватывающий все аспекты информационной безопасности взаимодействующих систем и других компонентов.

Шаблон документации, представленный в настоящем приложении, должен рассматриваться как пример построения шаблона документации.

А.2 Описание информационных систем и информационного обмена

В настоящем разделе должны быть объявлены цели и способы обмена информацией. Кроме того, все стороны должны описать в данном разделе свои информационные системы и другие компоненты, участвующие в информационном обмене.

А.3 Административный раздел шаблона документа

Формат документа может изменяться в зависимости от среды, в которой он будет использоваться. В одних случаях он может быть представлен в форме html-документов, в других — в бумажной форме. Настоящий формат, в который вставлены комментарии и пояснения, предназначен исключительно для того, чтобы проиллюстрировать составляющие, необходимые для создания эффективной документации, прилагаемой к соглашению.

Версия шаблона документа №. . . . . .

Дата: . . . . . .

Зона безопасности № 1

Лицо, ответственное за составление документа. . . . . .

Взаимодействующие системы: . . . . . .

. . . . . .

. . . . . .

Взаимодействующие приложения: . . . . . .

. . . . . .

. . . . . .

Рамки совместного доступа и ограничения доступа к информации:

. . . . . .

. . . . . .

Зона безопасности № 2

Лицо, ответственное за составление документа. . . . . .

Взаимодействующие системы: . . . . . .

. . . . . .

. . . . . .

Взаимодействующие приложения: . . . . . .

. . . . . .

. . . . . .

Рамки совместного доступа и ограничения доступа к информации:

. . . . . .

. . . . . .

А.4 Оценочный раздел шаблона документа

А.4.1 Схема классификации

Примеры классификаций, которые помогут при документировании систем, участвующих в информационном обмене.

Примеры вопросов, служащих для уточнения конкретных деталей, касающихся данного конкретного обмена информацией.

Очень важно, чтобы при организации обмена информацией в соответствии с настоящим стандартом обе стороны использовали одинаковые классификации и один и тот же набор вопросов. Это облегчает согласование документации всеми сторонами.

Также важно задокументировать как текущую ситуацию, так и ожидаемый/ необходимый уровень безопасности при передаче информации.

Такой способ документирования позволит выявить слабые стороны и другие проблемы с конфигурацией. Он также создает базис для взаимного соглашения сторон о том, что должно быть сделано для достижения надежной передачи информации, либо основу, на которой стороны смогут начать совместное использование информации с учетом известных проблем.

Каждая сторона заполняет вопросник. В шаблоне предусмотрены два столбца с ответами на каждый вопрос. Первый столбец озаглавлен «Текущее состояние», второй — «Согласовано». В первом столбце стороны должны ответить «да» или «нет» на вопрос о том, имеет ли их система определенные качества, или выбрать один из нескольких вариантов ответа, указанных в вопросе, соответствующий их системе. Во втором столбце стороны ставят отметку, если их система удовлетворяет политикам защиты обмена информацией, согласованным как для зоны 1, так и для зоны 2.

Категории защиты:

0 — не присвоена;

1 — несекретная;

2 — для служебного пользования;

3 — конфиденциальная;

4 — секретная;

5 — совершенно секретная.

А.4.2 Классификация подлежащей обмену информации по уровню защиты

А.4.2.1 Способ идентификации пациента	Текущее состояние	Согласовано
1 Фамилия, имя, отчество пациента		
2 Идентификационный номер пациента		
3 Фамилия, имя, отчество и идентификационный номер		
4 Иное (опишите):		

А.4.2.2 Способ идентификации медицинского работника	Текущее состояние	Согласовано
1 Фамилия, имя, отчество пациента		
2 Идентификационный номер пациента		
3 Фамилия, имя, отчество и идентификационный номер		
4 Иное (опишите):		

А.4.2.3 Способ получения информированного согласия пациента	Текущее состояние	Согласовано
1 Информированное согласие пациента не используется		
2 Информированное согласие пациента запрашивается		
3 Информированное согласие пациента запрашивается и проверяется пациентом		
4 Иное (опишите):		

А.4.2.4 Защита персональных данных пациента	Текущее состояние	Согласовано
1 Пациент не информирован об обмене данными		
2 Пациент информируется об обмене данными в устной форме		
3 Пациент получает письменную информацию об обмене данными		
4 Иное (опишите):		

А.4.2.5 Идентификация информации	Текущее состояние	Согласовано
1 Установлен ли метод обмена информацией?		

А.4.2.6 Локализация информации	Текущее состояние	Согласовано
1 Установлена ли процедура локализации, подлежащей обмену?		

А.4.2.7 Целостность информации

Идентификация передачи	Текущее состояние	Согласовано
1 Включен ли в сообщение идентификатор ответственного отправителя?		
2 Имеет ли каждое сообщение уникальный идентификатор?		
3 Шифруются ли данные при передаче?		
4 Регистрируется ли идентификатор ответственного получателя?		

А.4.2.8 Защита информации от искажения и/или изменения

Группы, предложенные ниже, представляют собой некоторые примеры анализа проблемы и могут быть изменены в зависимости от обстоятельств подготовки документации. Могут также группироваться различные сочетания для отражения местной ситуации.

Верификация передачи	Текущее состояние	Согласовано
1 Ведется ли журнал регистрации идентификаторов отправителя?		
2 Используется ли обратная передача данных для сравнения?		
3 Используется ли проверка контрольной суммы?		
4 Ведется ли регистрационный журнал идентификаторов лиц, подтверждающих получение сообщения?		
5 Ведется ли регистрационный журнал идентификаторов лиц, подтверждающих получение сообщения, и посылается уведомляющее сообщение отправителю?		

Класс прослеживаемости	Текущее состояние	Согласовано
1 Журнал передачи данных отсутствует		
2 Ведется журнал, подтверждающий, что передача данных имела место, без возможности восстановления переданных данных в случае потери		
3 Ведется журнал, подтверждающий, что передача данных имела место, с возможностью восстановления переданных данных в случае потери		
4 Верификация идентичности системы-отправителя		
5 Верификация идентичности системы-получателя		

А.4.3 Контрольные таблицы по безопасности

А.4.3.1 Примеры вопросов к отделу информационной безопасности	Текущее состояние	Согласовано
1 Имеются ли документированные требования к обеспечению безопасности и секретности данного обмена данными?		
2 Имеются ли документированные требования к правам доступа для данного типа обмена данными?		

А.4.3.2 Примеры вопросов к отделу эксплуатации системы	Текущее состояние	Согласовано
1 Имеется ли графическое представление системы и взаимодействующих компонентов для данного обмена информацией?		
2 Имеется ли защита от несанкционированного доступа к информации?		
3 Имеются ли антивирусные средства?		
4 Имеются ли соглашения, четко описывающие ответственность каждой стороны, обеспечивающей сопровождение системы?		
5 Имеются ли документированные регламенты отчетов о нарушениях и других проблемах при обмене информацией?		
6 Имеются ли документированные правила ужесточения ответственности, если после отчета о нарушении никакие меры не были приняты?		
7 Имеются ли документированные регламенты управления инновациями и изменениями системы и ее процессов?		
8 Имеются ли документированные регламенты резервного копирования, восстановления и архивирования?		
9 Имеются ли документированные средства и процедуры по регистрации происшествий?		
10 Имеются ли документированные правила установки исправлений и перехода на новые версии программного обеспечения?		
11 Имеются ли документированные альтернативные регламенты на случай неисправностей, продолжающихся длительное время?		

А.4.3.3 Примеры вопросов к владельцу системы	Текущее состояние	Согласовано
1 Имеется ли документация по функциям системы, используемым пользователем?		
2 Имеются ли четкое описание потоков данных между различными процессами и описание форматов транзакций обмена данными с другими системами?		
3 Имеется ли руководство пользователя системы?		
4 Имеются ли документированные регламенты оценки эффективности системы и получения предложений по ее улучшению?		
5 Имеются ли протоколы, правила принятия и документированные регламенты перехода на новую систему или на новую версию системы?		
6 Существуют ли специальные правила обращения с особо важной информацией?		

А.4.4 Административные контрольные таблицы

А.4.4.1 Авторизация	Текущее состояние	Согласовано
1 Используют ли обе стороны аналогичную структуру авторизации?		
2 Если нет, то существует ли схема полного отображения одной структуры на другую?		

А.4.4.2 Структура ролей	Текущее состояние	Согласовано
1 Используют ли обе стороны аналогичную структуру ролей?		
2 Если нет, то существует ли схема полного отображения одной структуры на другую?		

А.4.4.3 Делегирование прав	Текущее состояние	Согласовано
1 Имеют ли организации одинаковое делегирование прав?		
2 Если нет, то имеют ли организации полную схему отображения для делегирования прав?		

А.4.4.4 Период достоверности	Текущее состояние	Согласовано
1 Имеют ли организации одинаковую структуру периода достоверности?		
2 Синхронизируют ли организации периоды достоверности?		

А.4.4.5 Аутентификация пользователей/ролей	Текущее состояние	Согласовано
1 Применяют ли обе организации аутентификацию пользователей/ролей?		
2 Если да, идентичны ли системы аутентификации?		
3 Если нет, существует ли схема отображения аутентификаций, применяемых в системах?		

А.4.4.6 Доступ	Текущее состояние	Согласовано
1 Используются ли в обеих системах одинаковые роли для прав доступа?		
2 Если нет, то существует ли схема полного отображения между ролями для прав доступа, используемыми в системах?		

А.4.4.7 Срок действия соглашения (см. В.3.14)

А.4.4.8 Этические правила	Текущее состояние	Согласовано
1 Одинаковы ли в обеих организациях этические правила?		
2 Если нет, то существует ли схема отображения этических правил организаций?		

А.4.4.9 Защищенный регистрационный журнал	Текущее состояние	Согласовано
1 Используются ли в обеих организациях одинаковые правила ведения регистрационных журналов?		

А.4.4.10 Аудиторская проверка	Текущее состояние	Согласовано
1 Используют ли обе организации одинаковые правила относительно того, когда, кем и как анализируются записи регистрационных журналов?		

А.4.4.11 Анализ рисков	Текущее состояние	Согласовано
1 Используют ли обе организации одинаковые системы обнаружения рисков и управления ими?		
2 Если нет, то существует ли соглашение между организациями относительно того, как должны осуществляться обнаружение рисков и управление ими?		

А.4.4.12 Непрерывность и управление чрезвычайными ситуациями	Текущее состояние	Согласовано
1 Выработаны ли и согласованы обеими организациями общие правила и регламенты действий в случае сбоев?		

А.4.4.13 Развитие систем	Текущее состояние	Согласовано
1 Существует ли соглашение о развитии действующих систем?		

Приложение В
(справочное)

Пример соглашения о политике обмена информацией

В.1 Введение

Соглашение состоит из двух частей.

Первая часть является административной и определяет, какая информация подлежит обмену, какие медицинские структурные единицы участвуют в обмене, кто отвечает за обмен. В ней также указаны несоответствия требованиям генерального соглашения, требующие согласованного плана действий по их устранению.

Вторая часть представляет собой генеральное соглашение (соглашение о политике), касающееся всех аспектов обмена информацией между сторонами, определенных в В.2 и В.3.

В.2 Административная часть

В.2.1 Стороны соглашения

Сторона 1 _____

Сторона 2 _____

В.2.2 Область применения соглашения

Данное соглашение применяется к обмену информацией между вышеупомянутыми сторонами и другим вопросам, требующим урегулирования в соответствии с описанием, приведенным ниже.

В.2.3 Спецификация информации

Соглашение касается следующей информации:

_____

_____

_____

В.2.4 Контактные лица

Контактными лицами являются:

От Стороны 1

Фамилия, имя, отчество: _____

Телефон: _____ адрес электронной почты: _____

От Стороны 2

Фамилия, имя, отчество: _____

Телефон номер: _____ адрес электронной почты: _____

В.2.5 Примечания отдела информационной безопасности

Документация разработана: _____

_____

_____

Проверка безопасности осуществлена: _____

_____

_____

Подписано: _____

Дата передачи документации Стороне 1: ГГ-ММ-ДД _____

Дата передачи протокола проверки безопасности Стороне 1: ГГ-ММ-ДД _____

Срок проведения мероприятия 1: ГГ-ММ-ДД _____

Срок проведения мероприятия 2: ГГ-ММ-ДД _____

Срок проведения мероприятия N: ГГ-ММ-ДД _____

Дата передачи документации Стороне 2: ГГ-ММ-ДД _____

Дата передачи протокола проверки безопасности Стороне 2: ГГ-ММ-ДД _____

Срок проведения мероприятия 1: ГГ-ММ-ДД _____

Срок проведения мероприятия 2: ГГ-ММ-ДД _____

Срок проведения мероприятия N: ГГ-ММ-ДД _____

B.2.6 Другие вопросы

Следующие приложения являются неотъемлемой частью данного соглашения:

- приложение A Условия генерального соглашения;
- приложение B Общая документация;
- приложение C Протоколы проверки безопасности;
- приложение D Документ 1;
- приложение E Документ 2.

B.2.7 Подписи

Документ составлен в двух экземплярах — по одному для каждой стороны.

От Стороны 1

Дата: ГГ-ММ-ДД

От имени организации, ответственной за систему: _____

Ответственный за передаваемые данные: _____

Ответственный за систему: _____

От Стороны 2

Дата: ГГ-ММ-ДД

От имени организации, ответственной за систему: _____

Ответственный за передаваемые данные: _____

Ответственный за систему: _____

B.3 Пример содержания «Генерального соглашения о политике»

B.3.1 Область применения

B.3.1.1 Условия настоящего соглашения регулируют ответственность обеих Сторон при электронном обмене информацией.

B.3.1.2 При наличии отклонений от условий настоящего соглашения, эти отклонения должны быть определены в документе, приложенном к соглашению.

B.3.1.3 Условия настоящего соглашения составлены управлением информационных технологий или аналогичным органом и утверждены руководством организации.

B.3.2 Определения

B.3.2.1 Термин «Сторона» относится к тем, кто уполномочен использовать информационные системы и оборудование, определенные в настоящем соглашении, для электронного обмена информацией. Организация, ответственная за эксплуатацию систем и оборудования, применяемого для обмена информацией, также считается Стороной.

B.3.2.2 Термин «Информационная система» относится к местным информационным системам, коммуникационному оборудованию и другому цифровому оборудованию, необходимому для обработки, передачи, хранения и распечатки информации, определенной в настоящем соглашении.

В.3.2.3 Термин «Система» относится к совокупной системе, состоящей из систем и оборудования, участвующих в обмене информацией, определенном в настоящем соглашении.

В.3.2.4 Термин «Информация» относится к связной совокупности информации, определенной Сторонами в настоящем соглашении.

В.3.2.5 Термин «Анализ системы» относится к системе аудита, посредством которой все системы, участвующие в обмене информацией, проверяются на соответствие условиям, установленным уполномоченным лицом.

В.3.3 Система

В.3.3.1 Стороны должны провести тесты для проверки соответствия системы условиям, определенным в соглашении, и документировать результаты этих тестов. Документация должна быть создана обеими Сторонами в стандартизированной форме в соответствии с шаблоном документации, приведенном в приложении А.

В.3.3.2 До начала обмена информацией владелец системы должен протестировать информационные системы, участвующие в обмене, совместно с оператором системы.

В.3.3.3 Если в соглашении не указано иное, все затраты Сторон исчисляются с момента начала обмена информацией и работы системы.

В.3.3.4 Если в соглашении не указано иное, каждая Сторона должна с помощью тестов и других подходящих методов постоянно проверять, что система соответствует согласованным требованиям.

В.3.4 Обмен информацией

В.3.4.1 Если информация не может быть передана с помощью системы, виновная Сторона должна переслать информацию в соответствии с документированными альтернативными регламентами.

В.3.4.2 Информация, отличная от определенной в настоящем соглашении, не должна допускаться для передачи между системами без согласования Сторон и оператора систем.

В.3.4.3 Каждая Сторона несет ответственность за свою осведомленность о юридических нормах, применимых к настоящему соглашению, и за правильный обмен, обработку и хранение информации в соответствии с условиями настоящего соглашения.

В.3.5 Ответственность за местную информацию

Каждая Сторона несет ответственность за свой доступ к сертификатам и управление ими, а также за авторизацию подчиненного ей персонала.

В.3.6 Передача и получение информации

В.3.6.1 Информация считается переданной, когда акт передачи зарегистрирован в системном журнале обмена.

В.3.6.2 Информация считается принятой получающей Стороной, когда ее получение зарегистрировано в журнале получающей системы и она может быть прочитана получателем.

В.3.7 Информационная безопасность

В.3.7.1 Каждая Сторона должна гарантировать, что ее система выполняет необходимые требования информационной безопасности по защите самой информации и регистрационного журнала обмена информацией от несанкционированного доступа, искажения, задержек и потери данных.

В.3.7.2 Обязанностью каждой Стороны является проверка соответствия информационной системы, поставщика Интернет-услуг и/или средств передачи данных необходимым требованиям информационной безопасности по защите информации и регистрационного журнала обмена информацией от несанкционированного доступа, искажения, задержек и потери данных.

В.3.7.3 Содержание информации и ее отправитель должны допускать проверку надежным способом. Способ проверки должен быть определен в документации системы.

В.3.8 Конфиденциальность

В.3.8.1 Каждая Сторона должна трактовать информацию, коды доступа, имена пользователей и другую информацию по безопасности в соответствии с правилами своей организации и всеми возможными средствами пресекать попытки неавторизованных лиц получить доступ к этим сведениям.

В.3.8.2 Если Сторона получает данные, очевидно предназначенные третьей стороне, обязанностью получившей Стороны является немедленно задокументировать данный факт и сообщить об этом отославшей Стороне, а также, по возможности, связаться с предполагаемым получателем.

В.3.9 Доступность

В.3.9.1 Оператор системы обязан нести ответственность за выполнение согласованных запросов на доступ.

В.3.9.2 Каждая Сторона обязана нести ответственность за выполнение требований по доступу к информации, определенных в настоящем соглашении.

В.3.10 Информационные обязанности

В.3.10.1 Каждая Сторона обязана немедленно информировать другую Сторону о любых ситуациях, которые могут затруднить выполнение настоящего соглашения в течение краткого или длительного периода времени.

В.3.10.2 Каждая Сторона обязана участвовать в исследовании обновленной системы и осуществлении контроля по требованию оператора системы.

В.3.11 Архивирование

В.3.11.1 Каждая Сторона вместе с оператором системы несет ответственность за ведение полного журнала регистрации сообщений, переданных и полученных с помощью системы.

В.3.11.2 Каждая Сторона должна сохранять и резервировать информацию, доступную с помощью системы, в соответствии с законами, действующими на территории этой стороны. Если действующее законодательство не требует более длительного хранения, то информация должна храниться не менее трех лет. Хранение должно быть безопасным и не допускать несанкционированного доступа, искажения и потери информации. Сохраняемые данные должны быть доступны по первому требованию в читаемой форме в течение всего периода хранения.

В.3.11.3 Каждая Сторона обязана по требованию другой Стороны или тех, кого касается информация, предоставлять доступ к регистрационному журналу обмена информацией, а также к читаемым выдержкам из переданной информации.

В.3.12 Ответственность

В.3.12.1 Если не будет установлено намеренное или серьезное пренебрежение обязанностями, то ответственность за ущерб, причиненный одной из Сторон, должен ограничиваться компенсацией прямого ущерба, максимальный объем которой согласовывается Сторонами для каждого случая в настоящем соглашении.

В.3.12.2 Такая ограниченная ответственность применяется только к ущербу, вытекающему из настоящего соглашения, и не влияет на какие-либо другие соглашения Сторон или другие права Сторон, не подпадающие под действие настоящего соглашения.

В.3.13 Форс-мажорные обстоятельства

Стороны не несут ответственности за какие-либо задержки выполнения обязательств по настоящему соглашению, если могут доказать, что эти задержки вызваны обстоятельствами непреодолимой силы. Сторона также освобождается от ответственности перед другими Сторонами соглашения, если выполнение ее обязательств оказалось невозможным:

- по причине возникновения обстоятельств, неподконтрольных Стороне, и/или обстоятельств, которых Сторона не могла предвидеть или избежать;
- если Сторона не в состоянии выполнить эти обязательства по причине обстоятельств, вызванных третьей Стороной или стихийными бедствиями, бурей, молнией, пожаром, отсутствием электричества, забастовками, терроризмом, войной или другими беспорядками, а также изменением законодательства, включая сбои телекоммуникаций, дефицит услуг связи общего пользования, товаров, энергии или другие аналогичные обстоятельства.

В течение периода времени, когда Сторона находится под воздействием вышеупомянутых обстоятельств, другие Стороны обязаны выполнять свои обязательства перед этой Стороной в соответствии с этими условиями.

В.3.14 Срок действия соглашения

В.3.14.1 Сторона, подписавшая соглашение, может расторгнуть его, уведомив другую Сторону за 3 мес до срока прекращения действия.

В.3.14.2 Сторона, подписавшая соглашение, имеет право расторгнуть его немедленно, если другая Сторона признана виновной в существенном нарушении соглашения и не предпринимает попыток исправить такое нарушение в течение 30 дней с момента получения письменного запроса на расторжение соглашения.

В.3.14.3 Сторона, подписавшая соглашение, также имеет право расторгнуть его немедленно, если другая Сторона признается банкротом, иным способом выказывает несостоятельность или ликвидируется.

В.3.14.4 После аннулирования данного соглашения каждая из Сторон продолжает нести ответственность по обязательствам, связанным с обеспечением целостности информации и архивированием регистрационных журналов.

В.3.15 Изменения и дополнения

Руководящие органы организаций, к которым принадлежат Стороны, могут изменить условия генерального соглашения, за исключением пункта В.3.14. Такие изменения вступают в силу в течение 3 мес с момента получения письменного уведомления уполномоченным представителем другой Стороны. Если другая Сторона не принимает предложенных изменений, первая Сторона может в письменной форме потребовать расторжения соглашения с момента предполагаемого вступления в действие предложенных изменений. Изменения вступают в силу только при условии согласия обеих Сторон.

В.3.16 Передача третьей стороне

Ни одна из Сторон не имеет права передавать свои права и обязанности по настоящему соглашению третьей Стороне без согласия другой Стороны.

В.3.17 Споры

В.3.17.1 Споры, возникающие в связи с данным соглашением, должны в первую очередь разрешаться с помощью переговоров Сторон. Обе Стороны обязуются участвовать в таких переговорах в течение 30 дней с момента уведомления о возникновении спора.

В.3.17.2 Арбитражная комиссия должна разрешать разногласия Сторон, касающиеся настоящего соглашения таким же образом.

В.3.17.3 Стороны могут согласиться представить спор на рассмотрение предварительно согласованного лица или организации для вынесения принуждающего решения.

В.3.17.4 Если Стороны располагаются в разных странах, юрисдикция разрешения споров должна быть согласована Сторонами.

В.3.17.5 Споры, которые не могут быть разрешены путем переговоров, должны быть переданы в следующий суд:

(Наименование и адрес суда)

Библиография

[1] Blobel, B. and Roger-France, F., A Systematic Approach for Analysis and Design of Secure Health Information Systems, International Journal of Medical Informatics, 62 (3), pp. 51—78, 2001

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

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

[4] Ferraiolo, D.F., Sandhu, R., Gavrila, S., Kuhn, DR. and Chandramouli, R., Proposed NIST Standard for Role-Based Access Control, ACM Transactions on Information and System Security, 4 No. 3, August 2001, pp. 224—274

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

[6] ГОСТ Р ИСО 7498-2—99 Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации

[7] ISO/IEC 9594-8:2001, Information technology — Open Systems Interconnection — The Directory: Public-key and attribute certificate frameworks — Part 8

[8] ISO/IEC 9798-3:1998, Information technology — Security techniques — Entity authentication — Part 3: Mechanisms using digital signature techniques

[9] ISO/IEC 10181-1:1996, Information technology — Open Systems Interconnection — Security frameworks for open systems: Overview

[10] ISO/TS 17090-1:2002, Health informatics — Public key infrastructure — Part 1: Framework and overview

[11] ENV 13729:2000, Health informatics — Secure user identification — Strong authentication using microprocessor cards

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

[13] ENV 13606-3:2000, Health informatics — Electronic healthcare record communication — Part 3: Distribution rules

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

[15] ISO/TS 21298, Health informatics — Functional and structural roles

УДК 004:61:006.354 ОКС 35.240.80 П85 ОКСТУ 4002

Ключевые слова: здравоохранение, информатизация здоровья, обмен информацией, управление полномочиями, контроль доступа, управление политикой

Редактор *О.А. Стояновская*
Технический редактор *В.Н. Прусакова*
Корректор *В.Г. Гришунина*
Компьютерная верстка *И.А. Налейкиной*

Сдано в набор 09.09.2010. Подписано в печать 04.10.2010. Формат 60 × 84 1/8. Бумага офсетная. Гарнитура Ариал.
Печать офсетная. Усл. печ. л. 3,26. Уч.-изд. л. 2,70. Тираж 89 экз. Зак. 777.

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

gost.e-ecolog.ru