Утверждены
приказом и.о. Министра здравоохранения
Республики Казахстан
от «10» февраля 2014 года
№ 75

Технические требования к взаимодействию (передаче сообщений) с информационными системами е-здравоохранения

1.Общие положения

1. В данном Регламенте описаны основные требования по обеспечению конфиденциальности персональных медицинских данных в процессах е-Здравоохранения, разграничению прав доступа к электронным информационным ресурсам, содержащим персональные медицинские данные, а также порядок работы и взаимодействия ответственных лиц по защите информации.
2. Настоящие технические требования устанавливают требования к формату, составу и содержанию электронного сообщения, обеспечивающего информационное взаимодействие с центральными информационными системами е-Здравоохранения.
3. Порядок применения электронной цифровой подписи и (или) шифрования не относится к области применения настоящего Регламента, а рассматривается как «внешний» по отношению к нему и регламентируется отдельными документами.
4. Настоящие технические требования к взаимодействию (передачи сообщений) с информационными системами е-Здравоохранения разработаны в целях реализации «Концепции развития электронного здравоохранения Республики Казахстан на 2013-2020 годы», утвержденной приказом Министра здравоохранения Республики Казахстан от 3 сентября 2013 года № 498.
5. Настоящие технические требования определяет взаимодействие участников информационного обмена; правила интеграции с информационными системами пространства е-Здравоохранения, а также определяет требования к техническому обеспечению информационного обмена между информационными системами порядок, режимы работы и способы передачи данных.
6. Все информационные системы пространства е-Здравоохранения Республики Казахстан работают совместно и взаимодействуют на основе концепции СОА.
7. Способ доступа к информационным системам пространства е-Здравоохранения реализован в виде электронного сервиса.
8. Программно-аппаратные средства обеспечения защищенной интеграции информационных систем с интеграционной шиной обеспечивают выполнение настоящих Требований.

9. В настоящем документе использованы ссылки на следующие нормативные документы:

Кодекс Республики Казахстан «О здоровье народа и системе здравоохранения» от 18 сентября 2009 года № 193-IV;

Закон Республики Казахстан «Об информатизации» от 21 мая 2013 года № 94-V;

Закон Республики Казахстан «Об электронном документе и электронной цифровой подписи» от 7 января 2003 года № 370;

Постановление Правительства Республики Казахстан «Об утверждении Правил проведения аттестации государственных информационных систем и негосударственных информационных систем, интегрируемых с государственными информационными системами, на соответствие их требованиям информационной безопасности и принятым на территории Республики Казахстан стандартам» от 30 декабря 2009 года № 2280;

Стандарт Республики Казахстан ИСО/МЭК 27002-2009 – Информационные технологии. Средства обеспечения. Свод правил по управлению защитой информации;

Стандарт Республики Казахстан ИСО/МЭК 27001-2008 – Информационная технология. Методы и средства обеспечения. Системы управления информационной безопасностью. Требования;

Стандарт Республики Казахстан ИСО/МЭК 18028-4-2007 «Технологии информационные. Методы обеспечения защиты. Защита сети информационных технологий. Часть 4. Защита удаленного доступа»;

Стандарт Республики Казахстан ИСО/МЭК ТО 14516-2007 «Технологии информационные. Методы обеспечения защиты. Использование и управление услугами доверенной третьей стороны. Общие требования»;

Стандарт Республики 34.005–2002 – «Информационная технология. Основные термины и определения»;

Стандарт Республики Казахстан 34.006–2002 – «Информационная технология. Базы данных. Основные термины и определения»;

Стандарт Республики Казахстан 34.007–2002 – «Информационная технология. Телекоммуникационные сети. Основные термины и определения»;

Стандарт Республики Казахстан 34.013-2002 «Информационная технология. Защита информации от утечки по каналу побочных электромагнитных излучений и наводок при ее обработке на средствах вычислительной техники. Общие технические требования»;

Стандарт Республики Казахстан 34.023-2006 «Информационная технология. Методика оценки соответствия информационных систем требованиям безопасности»;

Стандарт Республики Казахстан 34.022-2006 «Защита информации. Требования к проектированию, установке, наладке, эксплуатации и обеспечению безопасности информационных систем»;

Стандарт Республики Казахстан 1073-2007. «Средства криптографической защиты информации»;

Международный стандарт HL7 (v3);

Международный стандарт DICOM.

10. В настоящем документе используются следующие основные термины и определения:

интеграционная шина – система, которая позволяет обеспечить взаимосвязь между информационными системами, а также обеспечить доступ к различным опубликованным сервисам, для использования, в соответствии с правилами СОА, информационными системами;

информационная система - система, предназначенная для хранения, обработки, поиска, распространения, передачи и предоставления информации с применением аппаратно-программного комплекса;

шлюз «электронного правительства» (далее - ШЭП) – информационная система, предназначенная для интеграции информационных систем «электронного правительства» в рамках реализации электронных услуг;

участник информационного обмена – информационные системы заинтересованных государственных органов и иных государственных организаций.

информационные технологии - совокупность методов, производственных процессов и программно-технических средств, объединенных в технологический комплекс, обеспечивающий сбор, создание, хранение, накопление, обработку, поиск, вывод, копирование, передачу и распространение информации;

реестр электронных сервисов - перечень сведений технических средств, обеспечивающих возможность электронного взаимодействия с информационными системами в соответствии с предъявляемыми требованиями;

паспорт электронного сервиса - документация предоставляемая поставщиком электронного сервиса для обеспечения информационного взаимодействия.

электронный информационный ресурс – технология его ведения и (или) использования, функционирующие в открытой информационно-коммуникационной сети, а также организационная структура, обеспечивающая информационное взаимодействие;

электронный сервис - идентифицируемая веб-адресом программная система со стандартизированными интерфейсами. Веб-сервисы могут взаимодействовать друг с другом и со сторонними приложениями посредством сообщений, основанных на специальных протоколах (например, SOAP);

электронное сообщение – информация, представленная в электронно-цифровой форме в формате XML (eXtensible Markup Language) и предназначена для обмена информацией между системами;

электронная цифровая подпись - набор электронных цифровых символов, созданный средствами электронной цифровой подписи и подтверждающий достоверность электронного документа, его принадлежность и неизменность содержания;

список отозванных регистрационных свидетельств (далее - СОРС) – электронный документ, созданный и подписанный НУЦ РК и содержащий информацию о регистрационных свидетельствах, выпущенных НУЦ РК, действие которых прекращено.

11. В настоящем документе использованы следующие обозначения и сокращения

СОА – сервис ориентированная архитектура;

ЭЦП – электронная цифровая подпись;

НУЦ РК - Национальный удостоверяющий центр Республики Казахстан;

SOAP — Simple Object Access Protocol – протокол обмена XML-сообщениями, имеющими определенную структуру; один из основных стандартов веб-сервисной технологии;

WSDL — Web Service Definition Language – стандарт описания интерфейсов веб-сервисов

XSD — это язык описания структуры XML документа.

XML — текстовый формат, предназначенный для хранения структурированных данных, для обмена информацией между программами, а также для создания на его основе более специализированных языков разметки.

HTTP (Hyper Text Transfer Protocol) - протокол прикладного уровня передачи данных (изначально — в виде гипертекстовых документов);

WSDL (Web Service Description Language) - стандартное определение вебсервиса;

WADL – (Web Application Description Language) - машинно-читаемое XML описание для HTTP web приложений (REST веб-сервисы).

UDDI (Universal Description Discovery&Integration) - спецификация универсального описания, поиска и интеграции электронных сервисов;

WS-Security (Web Services Security) - спецификация веб-сервисов, расширение SOAP для обеспечения безопасности веб-сервисов.

WS-Addressing - спецификация веб-сервисов, описывающая механизмы адресации транспортировки.

WS-Coordination - спецификация веб-сервисов, описывающая расширяемую инфраструктуру для предоставления протоколов, которые координируют действия распределенных приложений.

WS-Transaction - спецификация веб-сервисов, описывающая координации типов, которые используются с расширяемой основе для координации деятельности, описанных в спецификации WS-Coordination.

SSO (Single Sign-On) - технология единого входа - технология, при использовании которой пользователь переходит из одного раздела портала в другой без повторной аутентификации.

SAML (Security Assertion Markup Language) — язык разметки подтверждения безопасности) — основанный на языке XML стандарт, разработанный для обмена данными об аутентификации и авторизации между защищенными доменами.

camelCase— стиль написания составных слов, при котором несколько слов пишутся слитно без пробелов, при этом каждое слово пишется с заглавной буквы.

HL7 - HealthLevel 7 — стандарт обмена, управления и интеграции электронной медицинской информации.

IHEITI - Integrating the Healthcare Enterprise Information Technology Infrastructure – инфраструктура информационных технологий по интеграции предприятий здравоохранения;

CDAR2 – Clinical Document Architecture Release2 - Архитектура клинических документов релиз 2.

DICOM – Digital Imaging and Communications in Medicine - стандарт создания, хранения, передачи и визуализации медицинских изображений и документов обследованных пациентов, разработанный Национальной ассоциацией производителей электронного оборудования.

2.Требования к электронным сервисам

12. Электронные сервисы информационных систем участников взаимодействия должны соответствовать следующим основным спецификациям:

- спецификация UDDI;
- спецификация WSDL;
- спецификация протокола SOAP;
- спецификация формата XML;
- спецификация схем данных XSD;
- протокол передачи гипертекста HTTP.

13. При взаимодействии электронных сервисов с информационными системами е-Здравоохранения, а так же внешних информационных систем государственных органов, необходимо использовать следующие стандарты:

- WS – Security;
- WS – Addressing;
- SOAP;
- SSO/SAML;
- WSDL/ WADL;

- WS-Coordination / WS-Transaction;
- XML/XSL.

14. Для работы с электронными сервисами в пространстве е-Здравоохранения аутентификация должна осуществляться в соответствии с требованиями спецификации WS-Security.

15. Электронные сервисы, взаимодействующие с информационными системами е-Здравоохранения, должны удовлетворять следующим требованиям:

- все описания электронного сервиса и описания схем данных должны создаваться в кодировке UTF-8 или UTF-16 (с указанием этой кодировки в заголовке соответствующего описания);
- в описаниях электронного сервиса запрещены циклические ссылки между описаниями двух и более сервисов;
- однонаправленные ссылки между описаниями электронного сервиса и описаниями схем данных допустимы в любом количестве и сочетании;
- электронный сервис считается доступным, только при одновременной доступности точки доступа электронного сервиса;
- доступность электронного сервиса обеспечивает оператор информационной системы, в рамках которой функционирует электронный сервис (далее – поставщик электронного сервиса).

16. Электронные сервисы информационных систем участников взаимодействия могут разделяться по режиму работы в части обработки сообщений на синхронные и асинхронные электронные сервисы.

17. Электронные сервисы информационных систем участников взаимодействия должны обеспечивать гарантированную доставку неискаженных сообщений в рамках информационного обмена между информационными системами.

3.Требования к электронным сообщениям

18. Общая структура электронного сообщения включает в себя:

- заголовок электронного сообщения системы взаимодействия (soap: header);
- тело электронного сообщения системы взаимодействия (soap: body);
- сообщение об ошибке (soap: Fault).

19. Заголовок электронного сообщения системы взаимодействия включает в том числе:

- передачу сведений об аутентификации и авторизации (WS-security);
- передачу параметров при асинхронном взаимодействии (WS-Addressing).

20 Тело электронного сообщения системы взаимодействия в общем случае состоит из следующих элементов:

- блок данных;
- блок присоединенных документов;
- блок ЭЦП.

21. Блок данных электронного сообщения должен содержать дату и время отправки электронного сообщения в систему взаимодействия.

22. Блок присоединенных документов может содержать информацию (текстовую, графическую и пр.), прилагаемую к электронному сообщению системы взаимодействия.

23. Условия и порядок использования ЭЦП при осуществлении информационного взаимодействия определяются правилами Национального удостоверяющего центра Республики Казахстан в области применения ЭЦП.

24. Электронные сообщения,полученные по каналам связи, проходят контроль в следующем порядке:

- проверка ЭЦП электронного сообщения (обязательно);
- форматно-логическая проверка электронного сообщения.

25. При успешной проверке ЭЦП ИС НУЦ РК, производится проверка форматно-логического контроля электронного сообщения;

26. В случае, не прохождения проверки ЭЦП, электронное сообщение исключается из дальнейшей обработки, данный факт фиксируется в журнале.

27. Проверка форматно-логического контроля электронного сообщения производится информационной системой е-Здравоохранения, результат операции фиксируется в журнале.

28. В случае, не прохождения проверки форматно-логического контроля, электронное сообщение исключается из дальнейшей обработки, данный факт фиксируется в журнале.

29. В случае, прохождения проверки форматно-логического контроля электронного сообщения, отправителю направляется служебное электронное сообщение, извещающее об успешном приеме электронного сообщения.

4.Требования к метаданным

30. Все элементы метаданных в описании схемы данных должны быть документированы на государственном и русском языках.

31. Документирование элементов метаданных необходимо выполнять с использованием конструкции:

<xsd: annotation>

<xsd: documentation>Текст описания</xsd:documentation>
</xsd: annotation>

32. Синтаксическую конструкцию <!-- текст комментария --> рекомендуется применять только в качестве вспомогательных комментариев к описаниям данных, если это необходимо, и не использовать для документирования элементов метаданных.

33. При формировании наименования элементов метаданных рекомендуется осуществлять подбор слова или словосочетания из английского языка, соответствующего тому или иному используемому понятию.

34. Все слова в наименовании элемента метаданных необходимо использовать полностью, без сокращений. Слова должны записываться подряд, без пробела и других знаков между ними.

35. Наименования атрибутов метаданных должны записываться в стиле CamelCase: строчными буквами, кроме аббревиатур, записываемых полностью прописными (заглавными) буквами. Если используется два или более слова, то каждое последующее слово, кроме первого, должно начинаться с прописной (заглавной) буквы.

36. В наименования простых и составных типов (simple Type, complexType) для обозначения их отличия от элементов (element) необходимо добавлять суффикс «Type».

5.Требования к интеграционной шине

37. Информационный обмен между информационными системами е-Здравоохранения должен осуществляться посредством интеграционной шины, а также обеспечивать гарантированную доставку и целостность сообщений информационных систем.

38. Интеграционная шина должна обеспечивать:

- фиксацию факта доставки неискаженного сообщения либо факта ошибки при передаче сообщения;
- хранение сведений об истории движения электронных сообщений при предоставлении услуг;
- ведение журнала обращений потребителей к электронным сервисам.

39. Для взаимодействия с интеграционной шиной участник информационного взаимодействия должен:

- обеспечить защищенный канал связи для обмена электронными сообщениями;
- разработать интерфейсы взаимодействия в соответствии с требованиями настоящего документа;

- разработать паспорт электронного сервиса, регистрируемого в системе взаимодействия;
- разработать методику испытаний электронного сервиса, регистрируемого в системе взаимодействия, включая тестовый пример обращения к электронному сервису;
- разработать руководство пользователя электронного сервиса, регистрируемого в системе взаимодействия.

40. Электронные сервисы, обеспечивающие взаимодействие информационных систем с интеграционной шиной подлежат регистрации в реестре электронных сервисов.

6.Требования к регистрацииэлектронного сервиса

41. Электронные сервисы информационных систем участников взаимодействия подлежат регистрации в реестре электронных сервисов.

42. Регистрацию электронного сервиса осуществляет оператор интеграционной шины, в процессе которой осуществляется:
- проверка представленной документации;
- проверка соответствияразработанного электронного сервиса требованиям;
- тестирование электронного сервиса на тестовом примере в соответствии с представленной методикой испытаний.

43. Паспорт электронного сервиса, регистрируемый в системе взаимодействия, предоставляемый поставщиком указываются:
- полное и краткое наименование электронного сервиса;
- развернутое описание назначения электронного сервиса;
- информационная система, предоставляющая электронный сервис;
- стадия создания и использования электронного сервиса (разработка, тестовая эксплуатация, опытная эксплуатация или промышленная эксплуатация);
- режим гарантированной доступности электронного сервиса, который выражается в формате "a/b", где a - количество часов доступности сервиса в сутки; b - количество дней доступности сервиса в году, с дополнительным указанием рабочего времени;
- полное и сокращенное наименование организации - собственника технических средств, используемых для обработки информации, содержащейся в базах данных, составляющих информационную систему, предоставляющую электронный сервис;
- полное и сокращенное наименование организации - оператора информационной системы, предоставляющей электронный сервис;

- наименование структурного подразделения организации - оператора информационной системы, предоставляющей электронный сервис, ответственного за эксплуатацию сервиса;
- фамилия, имя, отчество (при наличии), должность, контактный телефон, адрес электронной почты должностного лица, ответственного за эксплуатацию электронногосервиса;
- текущая версия электронногосервиса в формате X.XX;
- тип режима работы электронногосервиса: A - асинхронный или C - синхронный;
- дата начала функционирования электронногосервиса;
- ссылка на документ, описывающий электронныйсервис;
- адрес электронного сервиса у поставщика;
- список кодов с наименованиями и описаниями ошибок, в случае их возникновения;

При заполнении паспорта электронного сервиса описание отдельных его элементов может повторяться.

44. При регистрации электронногосервиса в реестре электронных сервисов в паспорте электронного сервиса дополнительно указываются:
- неизменный уникальный идентификатор информационной системы в рамках принятой системы идентификации;
- неизменный уникальный идентификатор электронного сервиса в рамках принятой системы идентификации;
- узел системы взаимодействия;
- адрес электронногосервиса.

45. Регистрация электронногосервиса информационной системы поставщика и/или потребителя может считаться завершенной только при условии успешного выполнения тестового примера. Под тестовым примером обращения к электронному сервису понимается пример обращения к электронному сервису и ответа электронного сервиса на указанное обращение.

46. Назначением тестового примера является подтверждение работоспособности электронного сервиса при проведении процедуры регистрации, в рамках которой осуществляется отправка электронному сервису запроса, приведенного в тестовом примере, и сравнение полученного ответа с ответом, приведенным в тестовом примере.

47. Тестовый пример обращения и ответа должен быть предоставлен поставщиком в формате протокола обмена структурированными сообщениями.

48. Тестовый пример не должен вызывать выполнение каких-либо операций в информационной системе поставщика, которые могут привести к возникновению событий, позволяющих информационной системе интерпретировать полученные при выполнении тестового примера данные как реальные, а не тестовые.

49. Тестовый пример может быть использован для настройки модуля системы взаимодействия, обеспечивающего проверку доступности и работоспособности электронного сервиса, а также для отладки программного кода разработчиками потребителя электронного сервиса.

50. Регистрация электронного сервиса информационной системы поставщика и/или потребителя может считаться завершенной только при условии успешного выполнения тестового примера, которое предполагает совпадение ответа электронного сервиса с ответом, приведенным в тестовом примере.

51. Поставщик обеспечивает доступность электронного сервиса, регистрируемого для проведения приемки электронного сервиса.

52. В случае, если электронный сервис не проходит проверку, он возвращается на доработку разработчику электронного сервиса.

53. В случае, соответствия электронного сервиса условиям, указанным в Требованиях, оператор системы взаимодействия регистрирует его в реестре электронных сервисов.

54. При изменении программного кода электронного сервиса, зарегистрированного в интеграционной шине, поставщик электронного сервиса обеспечивает доступность новой версии электронного сервиса для проведения приемки и предоставляет оператору интеграционной шины следующие документы:

- паспорт новой версии электронного сервиса;
- методику испытаний новой версии электронного сервиса, включая тестовый пример обращения к электронному сервису;
- руководство пользователя новой версии электронного сервиса.

55. Оператор интеграционной шины осуществляет приемку новой версии электронного сервиса, разработанного поставщиком, в следующем порядке:

- проверяет комплектность и качество представленной документации;
- проверяет соответствие новой версии электронного сервиса предъявляемым требованиям;
- тестирует новую версию электронного сервиса на тестовом примере в соответствии с представленной методикой испытаний.

56. При положительных результатах проверки новой версии электронного сервиса, разработанного поставщиком, оператор интеграционной шиныосуществляет регистрацию электронного сервиса в интеграционной шине и рассылает уведомление всем потребителям данного электронного сервиса о выходе его новой версии и сроках работоспособности старой версии электронного сервиса.

57. В случае, если новая версия электронного сервиса, разработанного поставщиком, не прошла проверку, оператор интеграционной шины возвращает электронный сервис поставщику на доработку.

58. В целях, удаления из интеграционной шины ранее зарегистрированного электронного сервиса (далее - исключение электронного сервиса) поставщик направляет уведомление оператору интеграционной шинеоб исключении электронного сервиса с указанием причины.

59. Оператор интеграционной шины проверяет обоснованность заявки на исключение электронного сервиса из интеграционной шины и определяет оставшийся срок эксплуатации электронного сервиса.

60. Оператор интеграционной шины уведомляет потребителей электронного сервиса о сроках его отключения и удаляет электронный сервис из интеграционной шины. Поставщик выводит исключаемый электронный сервис из эксплуатации в установленный срок.

7.Требования к информационной безопасности

61. Информационная система, взаимодействующая с информационными системами е-Здравоохранения, должна соответствовать требованиям информационной безопасности согласно государственным стандартам Республики Казахстан (пункт 3 настоящего документа).

62. Все каналы связи, должны быть защищены с помощью сертифицированных средств криптографической защиты информации, соответствующих требованиям, установленным Стандартом Республики Казахстан 1073-2007. «Средства криптографической защиты информации».

63. Доступ третьих лиц ко всем техническим средствам, каналам связи и поддерживающим системам (электропитания, вентиляции, кондиционирования и т.п.) взаимодействия должен быть исключен.

64. Доступ к электронным сервисам информационных систем участников взаимодействия должен осуществляться с использованием сертифицированных средств межсетевого экранирования.

65. При взаимодействии с информационными системами е-Здравоохранения должна осуществляться идентификация и аутентификация информационных систем поставщиков и потребителей по идентификатору (коду) и паролю условно-постоянного действия длиной не менее восьми буквенно-цифровых символов или с использованием криптографических методов.

66. Программными средствами должны протоколироваться факты приема и отправки каждого информационного сообщения в рамках системы взаимодействия с указанием уникального в рамках электронного сервиса идентификатора сообщения, направления сообщения, даты, времени, адресата и контрольной суммы сообщения.

67. В рамках процедуры мониторинга состояния и использования электронных сервисов, зарегистрированных в интеграционной шине, для каждого взаимодействия автоматически должны регистрироваться следующие данные:

- запрашиваемый электронный сервис;
- пользователь (для авторизованных запросов);
- IP-адрес пользователя;
- время отклика электронного сервиса;
- содержимое запроса;
- содержимое ответа;
- объем передаваемых данных в запросе (в байтах);
- объем передаваемых данных в ответе (в байтах);
- при возникновении ошибки - ее описание.

68. В рамках процедуры мониторинга состояния и использования электронных сервисов, зарегистрированных в интеграционной шине, должны выполнять следующие действия:

- в автоматическом режиме осуществляется регулярный опрос зарегистрированных электронных сервисов, анализируется их состояние и формируется автоматическая рассылка уведомлений оператору системы взаимодействия и поставщику электронного сервиса при диагностировании ошибок;
- в автоматизированном режиме выполняются задачи предоставления аналитических отчетов по результатам работы интеграционной шины с возможностью группировки, сортировки и фильтрации данных.

69. Администрирование и сопровождение оборудования, обеспечивающего криптографическую защиту каналов связи, должно производиться только участником взаимодействия либо уполномоченными им лицами.

70. В целях обеспечения защиты информации, содержащейся в информационных системах, подключенных к системе взаимодействия, участники информационного взаимодействия:

- обеспечивают при обслуживании информационных систем, подключенных к интеграционной шине, исполнение установленных требований по информационной, производственной, технологической и противопожарной безопасности;
- осуществляют контроль доступа посторонних лиц к техническим средствам и каналам связи в контролируемой зоне участника взаимодействия, включая время проведения ремонтных работ и уборки помещений;
- обеспечивают обслуживание информационных систем, подключенных к интеграционной шине, только лицами, имеющими право доступа к информации, содержащейся в указанных информационных системах;
- принимают необходимые и достаточные меры, исключающие доступ посторонних лиц к защищаемой информации, в том числе парольной и ключевой информации, хранящейся на используемых и отчуждаемых носителях информации;
- осуществляют учет лиц, имеющих доступ к конечному оборудованию, обеспечивающему криптографическую защиту каналов связи интеграционной шины, расположенной в контролируемой зоне участника взаимодействия, а также лиц, имеющих возможность изменения конфигурации информационных систем данного участника взаимодействия, подключенных к интеграционной шине.

71. В целях обеспечения полноценного функционирования интеграционной шины и подключенных к ней информационных систем каждый участник взаимодействия:

- обеспечивает возможность оперативного переключения на резервный канал с сохранением функций обеспечения безопасности информации для всех каналов связи, выход из строя которых может существенно повлиять на доступность информационных систем, подключенных к интеграционной шине;
- обеспечивает возможность оперативной замены оборудования, обеспечивающего криптографическую защиту каналов связи, используемых участником взаимодействия для осуществления информационного обмена в рамках интеграционной шины, в случае выхода такого оборудования из строя.

72. В целях обеспечения конфиденциальности информации о пациенте, целости данных и учета действий пользователей, а также мониторинга предоставления электронной медицинской информации персональных данных между медицинскими информационными системами и центральными системами должны использоваться соответствующие профили и транзакции IHE ITI .

8.Требования взаимодействия с центральными системами е-Здравоохранения

73. Обмен сообщениями электронной медицинской информации информационных систем с центральными системами е-Здравоохранения должен осуществляться в соответствии с требованиями международного стандарта HL7 версии 3.

74. Хранение и передача документов электронной медицинской информации в репозитории системы должен осуществляться в соответствии с требованиями архитектуры клинического документа стандарта HL7 CDA R2.

75. Создание, хранение, передача и визуализации медицинских изображений осуществляться в соответствии с требованиями отраслевого стандарта DICOM.

76. Координация процессов обмена электронной медицинской информации между информационными системами и центральными системами должны использоваться соответствующие профили и транзакции IHE ITI.