|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | ЕДИНАЯ ГОСУДАРСТВЕННАЯ ИНФОРМАЦИОННАЯ СИСТЕМА В СФЕРЕ ЗДРАВООХРАНЕНИЯ  ПОяснительная записка к системному проекту  Книга 2 Решения по развитию прикладных информационных систем, входящих в ЕГИСЗ  Раздел 1 Основные технические требования к прикладным информационным системам, входящим в состав ЕГИСЗ | | | |
|  | | | |
|  | | | |
|  | |  | |
|  | | | |
|  |  |  | |  |

**Содержание**

Аннотация 3

Перечень принятых сокращений 5

Перечень принятых терминов и определений 11

1 Основные технические требования к прикладным информационным системам, входящим в состав ФС ЕГИСЗ 13

1.1 Текущий состав ФС ЕГИСЗ и смежных систем 13

1.1.1 Компоненты ФС ЕГИСЗ 13

1.1.1.1 Интегрированная электронная медицинская карта (ИЭМК) 15

1.1.1.2 Федеральная электронная регистратура (ФЭР) 17

1.1.1.3 Компонент информатизации административно-хозяйственной деятельности (АХД) 19

1.1.1.4 Информационно-аналитическая система принятия управленческих решений (ИАС УР) 19

1.1.1.5 Единая система идентификации, аутентификации и авторизации пользователей (ЕСИАиА) 22

1.1.1.6 Система интеграции прикладных систем (ИПС) 24

1.1.1.7 Система ведения нормативно-справочной информации (Система НСИ) 25

1.1.2 Принципы интеграции компонентов ЕГИСЗ с внешними информационными системами 26

1.1.3 Базовые требования к взаимодействию с внешними информационными системами 28

1.2 Технические требования к информационным системам ландшафта ФС ЕГИСЗ 36

1.2.1 Требования к масштабируемости ФС ЕГИСЗ 38

1.2.2 Требования к расширению функциональных возможностей ФС ЕГИСЗ 39

1.2.3 Требования к изменению уровня безопасности Системы 42

1.2.4 Требования к защите информации от несанкционированного доступа 43

1.2.5 Перечень аварийных ситуаций 46

1.2.6 Требования к надежности технических средств и программного обеспечения ФС ЕГИСЗ 48

1.3 Описание технических требованиям к информационным сервисам в рамках развития компонентов ФС ЕГИСЗ 49

1.3.1 Технические требования к развитию сервиса ФЭР 49

1.3.2 Технические требования к развитию сервиса ИАС УР 49

1.3.3 Технические требования к развитию Системы НСИ 50

1.3.4 Технические требования к развитию сервиса ИЭМК 51

1.3.5 Технические требования к функционированию РИП ММД 51

# Аннотация

Настоящий документ (Книга 2) посвящен определению наиболее оптимальных решений по развитию прикладных информационных систем, входящих в состав федерального сегмента (ФС) ЕГИСЗ. Книга состоит из восьми разделов в которых рассмотрен текущий состав ФС ЕГИСЗ и смежных систем, определены требования к информационным системам, входящим в ФС ЕГИСЗ и порядок их интеграции, предложены целесообразные системотехнические решения по развитию основных функциональных компонент ФС ЕГИСЗ.

В Разделе 1 описаны основные технические требования к прикладным информационным системам, входящим или планируемым к вхождению в ФС ЕГИСЗ. Особое внимание уделено принципам интеграции компонентов ФС ЕГИСЗ с внешними информационными системами, техническим требованиям к информационным системам ландшафта ФС ЕГИСЗ, описанию технических требованиям к информационным сервисам в рамках развития компонентов ФС ЕГИСЗ.

В Разделах 2-7 даются в развернутом виде системотехнические решения по развитию всех основных существующих компонент ФС ЕГИСЗ, таких как:

* Единая подсистема идентификации, аутентификации и авторизации пользователей ЕГИСЗ на основе ЕСИАиА – Раздел 2,
* Федеральная электронная регистратура. Система ведения расписания приемов специалистов, проведения консультаций, в том числе телемедицинских, и загрузки мощностей медицинской организации, а также электронной записи на прием к врачу, с учетом возможности интеграции с внешними информационными системами с использованием облачных технологий (ФЭР) – Раздел 3,
* Система ведения интегрированной электронной медицинской карты (ИЭМК) – раздел 4,
* Система, обеспечивающая управленческий учет административно-хозяйственной деятельности медицинских организаций, в том числе автоматизирующей функции взаимодействия со страховыми медицинскими организациями в части формирования и оплаты счетов за оказанную медицинскую помощь, и управленческий кадровый учет в медицинских организациях, на основе существующих федеральных управленческих систем с использованием облачных технологий (АХД) – Раздел 5,
* Информационно-аналитическая подсистема Минздрава России в части поддержки принятия управленческих решений на основе данных мониторинга, регистровых данных и данных первичного учета в здравоохранении (ИАС УР) – Раздел 6,
* Программный комплекс «Реестр нормативно-справочной информации системы здравоохранения» - Раздел 7.

В Разделах 2-7 дано подробное описание сервисов по результатам первой очереди создания ФС ЕГИСЗ, их текущее состояние, определены и обоснованы наиболее целесообразные пути функционального и технологического развития сервисов.

В Разделе 8 даны основные системотехнические решения по созданию сервиса обеспечения функции диспетчеризации санитарного автотранспорта. В связи с тем, что это новый сервис в составе ФС ЕГИСЗ, особое внимание в разделе уделено обоснованию и цели создания сервиса, здесь подробно описаны архитектурные решения, которые должны быть заложены при создании соответствующей компоненты, определены и обоснованы требования к функциональности сервиса.

Перечень принятых сокращений

| Сокращение | Расшифровка сокращения |
| --- | --- |
| АРМ | Автоматизированное рабочее место |
| АХД | Компонент ФС ЕГИСЗ, обеспечивающий управленческий учет административно-хозяйственной деятельности медицинских организаций, в том числе автоматизирующей функции взаимодействия со страховыми медицинскими организациями в части формирования и оплаты счетов за оказанную медицинскую помощь, и управленческий кадровый учет в медицинских организациях, на основе существующих федеральных управленческих систем с использованием облачных технологий |
| ГОСТ | Государственный стандарт |
| ГРЛС | Государственный реестр лекарственных средств |
| ЕГИСЗ | Единая государственная информационная система в сфере здравоохранения |
| ЕПГУ | Единый портал государственных и муниципальных услуг |
| ЕРЗ ФОМС | Единый регистр застрахованных граждан ФОМС |
| ЕСИА | Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме |
| ЕСИАиА | Компонент ЕГИСЗ. Единая подсистема идентификации, аутентификации и авторизации пользователей ЕГИСЗ на основе ЕСИА |
| ИАС УР | Компонент ФС ЕГИСЗ. Информационно-аналитическая подсистема Минздрава России в части поддержки принятия управленческих решений на основе данных мониторинга, регистровых данных и данных первичного учета в здравоохранении |
| ИС | Информационная система |
| ИЭМК | Интегрированная электронная медицинская карта |
| ЛВС | Локально вычислительная сеть |
| МИС | Медицинская информационная система |
| МО | Медицинская организация |
| МП | Медицинская помощь |
| НСД | Несанкционированный доступ |
| НСИ | Нормативно-справочная информация |
| ОГРН | Основной государственный регистрационный номер |
| ОУЗ | Орган управления здравоохранением |
| ПО | Программное обеспечение |
| Реестр НСИ | Программный комплекс «Реестр нормативно-справочной информации системы здравоохранения» |
| РИП ММД | Распределенное информационное пространство медицинских мультимедийных данных |
| РС ЕГИСЗ | Региональный сегмент единой государственной информационная система в сфере здравоохранения |
| РФ | Российская Федерация |
| Сервис ИПС | Компонент "Сервис интеграции прикладных систем". Общесистемный технологический сервис, входящий в состав сегмента централизованных общесистемных компонентов ФС ЕГИСЗ |
| Система ведения ИЭМК | Компонент ФС ЕГИСЗ по ведению интегрированной электронной медицинской карты и сервисах доступа к ней с использованием сервисно-ориентированных и облачных технологий, входящей в состав ФС ЕГИСЗ Минздрава России |
| СМ | Система мониторинга |
| СМО | Страховая медицинская организация |
| СМЭВ | Система межведомственного электронного взаимодействия |
| СНИЛС | Страховой номер индивидуального лицевого счета застрахованного лица в системе персонифицированного учета Пенсионного фонда Российской Федерации |
| СПО | Программное обеспечение, распространяемое под свободной лицензией |
| СУБД | Система управления базами данных |
| СЭМД | Стандартизированный электронный медицинский документ |
| ТАП | Талон амбулаторного посещения |
| ТЗ | Техническое задание |
| УЗ | Учреждение здравоохранения |
| ФГИС | Федеральная государственная информационная система |
| ФЛК | Форматно логический контроль |
| ФО | Федеральный округ |
| ФОМС | Фонд обязательного медицинского страхования |
| ФРМП | Подсистема «Федеральный регистр медицинского персонала» Информационно-аналитической системы Минздрава России |
| ФС ЕГИСЗ | Федеральный сегмент единой государственной информационная система в сфере здравоохранения |
| ФСС | Фонд социального страхования Российской Федерации |
| ФЦОД | Федеральный центр обработки данных |
| ФЭР | Компонент ФС ЕГИСЗ. Федеральная электронная регистратура. Система ведения расписания приемов специалистов, проведения консультаций, в том числе телемедицинских, и загрузки мощностей медицинской организации, а также электронной записи на прием к врачу, с учетом возможности интеграции с внешними информационными системами с использованием облачных технологий |
| ХД | Хранилище данных |
| ЦОД | Центр обработки данных |
| ЭМК | Электронная медицинская карта |
| ЭП | Электронная подпись |
| API | Application programming interface - интерфейс программирования приложений |
| ATNA | Audit Trail and Node Authentication (IHE) – профиль поддержки аудита доступа и аутентификация узла |
| Call-центр | Центр обслуживания звонков |
| CDA | Clinical Document Architecture – архитектура клинических документов. Стандарт ISO/HL7 27932:2009 Data Exchange Standards -- HL7 Clinical Document Architecture, Release |
| ESB | Enterprise Service Bus - сервисная шина предприятия. Подход к построению распределённых корпоративных информационных систем, включающий в себя промежуточное ПО, которое обеспечивает взаимосвязь между различными приложениями по различным протоколам взаимодействия |
| HL7 | Health Level Seven - стандарт обмена, управления и интеграции электронной медицинской информации |
| HTML | Hyper-Text Markup Language – язык гипертекстовой разметки |
| IHE | Integrating the Healthcare Enterprise - международная инициатива, направленная на адаптацию и использование стандартов в области информатизации здравоохранения разработчиками медицинских информационных систем и медицинского оборудования |
| MIME | Multipurpose Internet Mail Extensions – стандарт, описывающий передачу различных типов данных по электронной почте, а также, шире, спецификация для кодирования информации и форматирования сообщений таким образом, чтобы их можно было пересылать по Интернет |
| PDF | Portable Document Format – платформонезависимый формат электронных документов, созданный фирмой Adobe Systems использованием ряда возможностей PostScript |
| PDQ | The Patient Demographics Query (IHE) – профиль поддержки поиска идентификатора пациента в заданной медицинской организации и его «демографических» данных по заданным критериям |
| PIX | Patient Identifier Cross-Referencing (IHE) - профиль поддержки однозначной идентификации пациента, идентификационные данные которого находятся в различных медицинских учреждениях, путём корректного сопоставления множества идентификаторов |
| SaaS | Software as a Service – программное обеспечение как сервис |
| SOA | Сервис-ориентированная архитектура (англ. Service-oriented Architecture) – модульный подход к разработке программного обеспечения, основанный на использовании распределённых, слабо связанных заменяемых компонентов, оснащённых стандартизированными интерфейсами для взаимодействия по стандартизированным протоколам |
| SOAP | Simple Object Access Protocol - простой протокол доступа к объектам |
| WSDL | Web Services Description Language – язык описания веб-сервисов и доступа к ним, основанный на языке XML |
| XDS | Cross-Enterprise Document Sharing (IHE) – профиль доступа к медицинским документам, хранящимся в системе |
| XDS.b | Cross-Enterprise Document Sharing-b (IT Infrastructure Technical Framework, IHE) – профиль поддержки публикации, хранения и доступа к медицинским документам |
| XML | eXtensible Markup Language - расширяемый язык разметки, текстовый формат, предназначенный для хранения структурированных данных и для обмена информацией между программами |
| XSD | Схема документа в формате XML (англ: XML Schema) – язык описания структуры XML-документа |

Перечень принятых терминов и определений

| **Термин** | **Определение** |
| --- | --- |
| Авторизация | Предоставление определённому лицу или группе лиц прав на выполнение определённых действий; а также процесс проверки (подтверждения) данных прав при попытке выполнения этих действий |
| Аутентификация | Процедура проверки подлинности, например: проверка подлинности пользователя путём сравнения введённого им пароля с паролем в базе данных пользователей |
| Идентификация | Процедура, в результате выполнения которой для субъекта идентификации выявляется его идентификатор, однозначно идентифицирующий данный субъект в информационной системе |
| Концепция | Концепция создания единой государственной информационной системы в сфере здравоохранения, утвержденная приказом Минздравсоцразвития России от 28.04.2011 № 364 «Об утверждении Концепции создания единой государственной информационной системы в сфере здравоохранения» |
| Медицинская запись | Электронная персональная медицинская запись: любая персональная медицинская запись, сохраненная на электронном носителе (ГОСТ Р 52636-2006 «ЭЛЕКТРОННАЯ ИСТОРИЯ БОЛЕЗНИ.ОБЩИЕ ПОЛОЖЕНИЯ»).  Персональная медицинская запись: любая запись, сделанная конкретным медицинским работником в отношении конкретного пациента (ГОСТ Р 52636-2006 «ЭЛЕКТРОННАЯ ИСТОРИЯ БОЛЕЗНИ. ОБЩИЕ ПОЛОЖЕНИЯ»). Объект учёта Системы ведения ИЭМК, объединяющий параметры, регистрируемые при оказании медицинской услуги |

# Основные технические требования к прикладным информационным системам, входящим в состав ФС ЕГИСЗ

## Текущий состав ФС ЕГИСЗ и смежных систем

### Компоненты ФС ЕГИСЗ

Федеральный сегмент ЕГИСЗ представляет собой комплексную информационную систему, решающую задачи по повышению качества и доступности медицинской помощи гражданам. В состав ФС ЕГИСЗ входят различные системы, которые обеспечивают исполнение сквозных процессов и реализуют принципы, описанные в Концепции создания единой государственной информационной системы в сфере здравоохранения, утвержденной приказом Минздравсоцразвития России от 28.04.2011 № 364 «Об утверждении Концепции создания единой государственной информационной системы в сфере здравоохранения». Взаимодействие систем строится на базе единых правил с использованием единых справочников. Для построения такой сложной системы необходимо унифицировать технические требования к составу данных, протоколов и правил передачи информации как для компонентов Системы, разработанных на первом этапе ее создания, так и в целях дальнейшего развития ФС ЕГИСЗ.

При разработке правил взаимодействия системных компонентов необходимо принимать во внимание требования уже используемых и разрабатываемых государственных сервисов и реализованную между ними интеграцию, а также методических рекомендаций по разработке электронных сервисов.



Рисунок 1 - Целевая схема ФС ЕГИСЗ

#### Интегрированная электронная медицинская карта (ИЭМК)

Данный сервис разрабатывается в целях обеспечения непрерывности, преемственности и качества лечения, своевременной профилактики и иных мероприятий по обеспечению здоровья конкретного гражданина путем документирования и сохранения соответствующей медицинской информации и своевременного предоставления ее уполномоченным медицинским работникам и организациям, а также субъектам ИЭМК. Основным поставщиком информации для ИЭМК являются региональные транзакционные сервисы ведения ЭМК (как независимые сервисы или как компоненты МИС).

ИЭМК содержит персонифицированные демографические данные и сведения о здоровье гражданина, планах лечения, назначениях и результатах лечебных, диагностических, профилактических, реабилитационных, санитарно-гигиенических и других мероприятий, однако информация, содержащаяся в ИЭМК, может быть обезличена.

ИЭМК должна обеспечивать безбумажную обработку данных в распределенной многопользовательской среде. Данные, предоставляемые в ИЭМК, должны подписываться электронной подписью (в терминах Федерального закона от 27.07.2006 г.№ 152-ФЗ «О персональных данных» с учетом последних редакций).

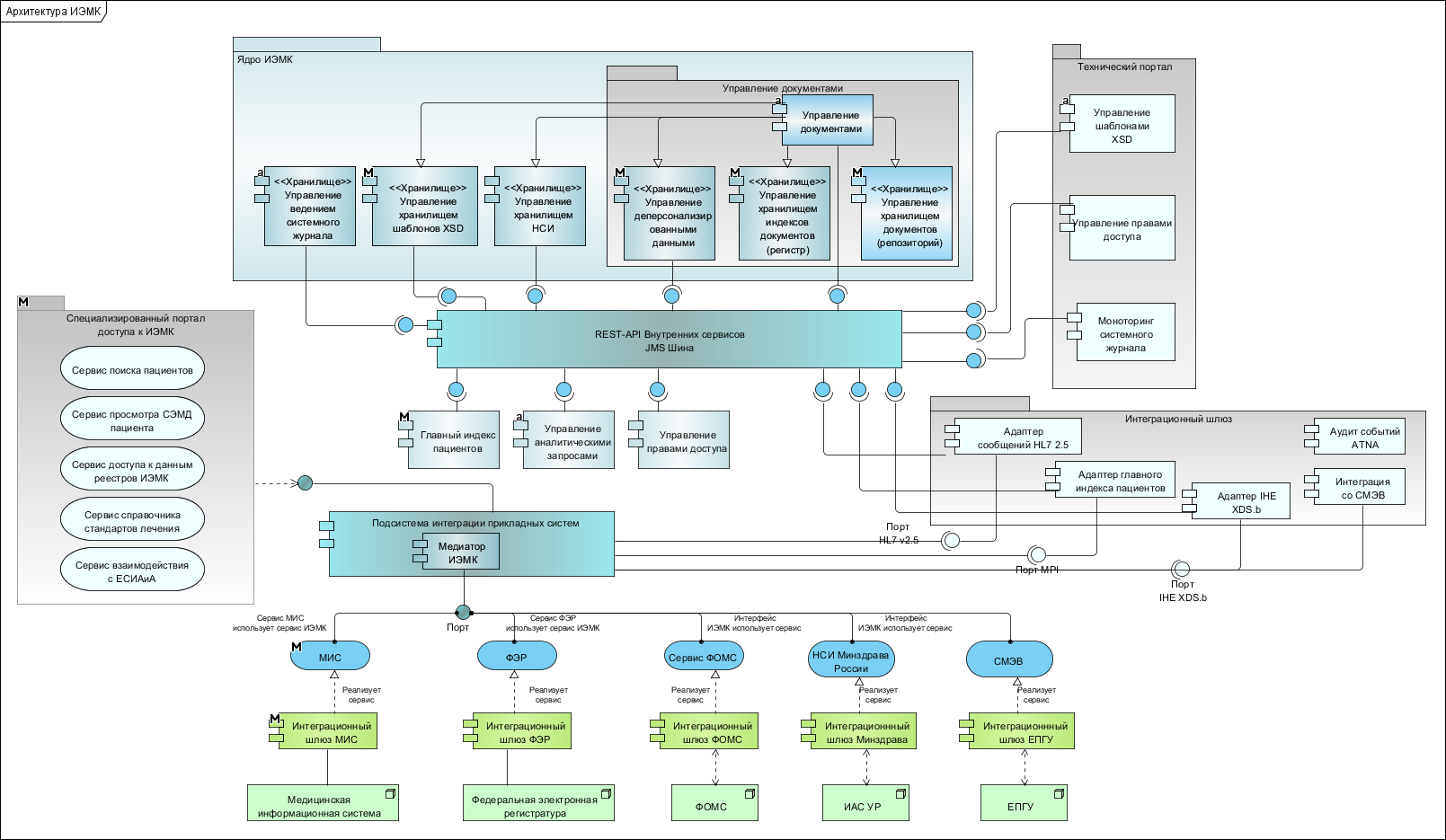


Рисунок 2 - Структурная схема ИЭМК

Интеграционные профили ИЭМК предназначены для обмена информации с внешними ИС и состоят из следующих модулей:

* выгрузки, хранения и предоставления доступа к ИЭМК;
* обеспечения доступа к ИЭМК через веб-сервисы;
* аудита в части взаимодействия;
* работы с идентификаторами пациентов;
* интеграции с ЕРЗ ФФОМС;
* интеграции со СМЭВ;
* интеграции с Реестром НСИ.

#### Федеральная электронная регистратура (ФЭР)

Данный сервис разрабатывается для реализации возможности ведения расписания приемов специалистов, проведения консультаций, в том числе телемедицинских, загрузки мощностей медицинской организации, а также электронной записи на прием к врачу. Разработка ФЭР проведена с учетом требований к интеграции с внешними информационными системами на принципах использования облачных технологий.

Сервис является приемником и поставщиком данных для региональных информационных систем ведения расписаний, ИЭМК, различных регистров и учетных систем.

ФЭР в качестве компонента ФС ЕГИСЗ является инструментом для управления ресурсами отрасли здравоохранения, оптимизации использования ресурсов, контроля и аналитики. Также стоит отметить важную роль данного компонента в повышении доступности медицинской помощи и в предоставлении возможности гражданам выбирать место и время получения медицинской помощи.

Интеграционные профили ФЭР предназначены для обмена информации с внешними ИС и состоят из следующих модулей:

* Интеграции с модулем ведения электронного расписания в МИС регионального сегмента;
* Интеграции с ИЭМК;
* Предоставления доступа к ФЭР;
* Аудита в части взаимодействия;
* Интеграции с ЕРЗ ФФОМС;
* Интеграции со СМЭВ;
* Интеграции с Реестром НСИ;
* Интеграции с системами АХД, а также с регистрами.



Рисунок 3 - Структурная схема ФЭР

#### Компонент информатизации административно-хозяйственной деятельности (АХД)

Сервис реализуется для целей обеспечения учета административно-хозяйственной деятельности медицинских организаций, в том числе -автоматизации функций взаимодействия со страховыми медицинскими организациями (в части формирования и оплаты счетов за оказанную медицинскую помощь), управленческого кадрового учета в медицинских организациях на основе существующих федеральных управленческих систем с использованием облачных технологий.

#### Информационно-аналитическая система принятия управленческих решений (ИАС УР)

Данный компонент представляет собой информационно-аналитический сервис Минздрава России, обеспечивающий поддержку принятия управленческих решений на основе данных мониторинга и регистровых данных первичного учета в здравоохранении. Информационная система работает с различными данными, полученными из транзакционных систем всего контура ФС ЕГИСЗ, и позволяет управлять качеством медицинской помощи, отслеживать и анализировать тренды в здравоохранении, получать необходимую отчетность без дополнительных запросов в медицинские организации.

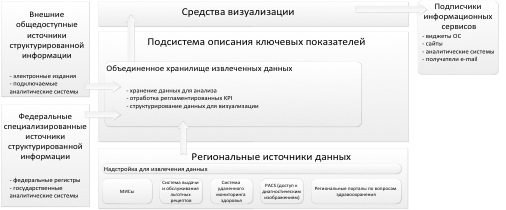


Рисунок 4 - Компонентная модель ИАС УР

Основными функциями, выполняемыми ИАС УР, являются:

* сбор данных учета и мониторинга на уровне МО, обеспечивающего возможность формирования настраиваемой отчетности на основе единой, унифицированной для всех регионов, структуры медицинских данных и ключевых индикаторов, определяемой на федеральном и/или региональном уровне;
* ведение федерального хранилища псевдонимизированных данных и данных, агрегированных на уровне МО;
* ведение перечня ключевых индикаторов в сфере здравоохранения, включая ключевые индикаторы реализации целевых программ, а также ключевые индикаторы деятельности медицинских учреждений и регламентов автоматизированного сбора данных, необходимых для их расчета;
* сбор первичных данных персонифицированного учета оказанной медицинской помощи и лекарственного обеспечения, а также псевдонимизированных данных, содержащихся в интегрированной электронной медицинской карте;
* план-факт анализ данных ключевых индикаторов в сфере здравоохранения;
* информационное взаимодействие с иными федеральными информационными системами и ресурсами;
* информационное взаимодействие со сторонними региональными информационными системами;
* информационное взаимодействие с системой мониторинга реализации региональных программ модернизации здравоохранения;
* интеграция со следующими компонентами ЕГИСЗ:
* каталог пользователей ЕГИСЗ (поддержка Single Sign On в рамках объединенного информационного пространства ЕГИСЗ);
* подсистема ведения НСИ и словарей медицинских терминологий ЕГИСЗ;
* инфраструктура открытых ключей ЭП ЕГИСЗ.

Программное обеспечение ИАС УР включает в себя компоненты, реализующие функциональные подсистемы:

* Централизованное хранилище данных для поддержки принятия управленческих решений на основе данных первичного учета;
* Подсистема сбора, консолидации и обработки транзакционных данных медицинских информационных систем (данных первичного учета в здравоохранении);
* Подсистема описания ключевых показателей для поддержки принятия управленческих решений;
* Подсистема анализа, мониторинга и контроля для поддержки принятия управленческих решений на основе данных первичного учета в здравоохранении;
* Подсистема визуализации данных для регионов в части поддержки принятия решений (основанная на первичных данных, включая данные из медицинских информационных систем);
* Подсистема информационного обмена (в части взаимодействия с региональными медицинскими информационными системами);
* Подсистема разграничения прав доступа (в части организации регламентированного доступа пользователей к функциям, связанным с поддержкой принятия решений).

При передаче сообщений осуществляется форматно-логический контроль сообщений. Алгоритм контроля задается на этапе проектирования логики работы системы.

Форматно-логический контроль должен осуществляться на этапе передачи информации сервисом – приемником информации. Правила для такого контроля задаются на этапе разработки для обеспечения непротиворечивости и качества информации. Форматно-логический контроль также применим для сообщений, подписанных ЭП, заключающийся в проверке валидности формата и служебной информации сообщения, необходимой для его доставки и маршрутизации в рамках среды СМЭВ.

#### Единая система идентификации, аутентификации и авторизации пользователей (ЕСИАиА)

Единая система идентификации, аутентификации и авторизации пользователей создается для обеспечения санкционированного доступа субъектов информационного взаимодействия (граждан и должностных лиц МО, ОУЗ) к информации, содержащейся в ЕГИСЗ, основываясь на правилах безопасности, настроенных для каждой из систем информационного ландшафта ЕГИСЗ, участвующей в информационном взаимодействии.

При этом надо заметить, что доступ к компонентам Системы на базе ролей пользователей осуществляется непосредственно в информационных системах.

ЕСИАиА обеспечивает санкционированный доступ участников информационного взаимодействия (заявителей и должностных лиц МО, ОУЗ) к информации, содержащейся в ЕГИСЗ.

Основные функциональные возможности ЕСИАиА:

* Идентификация и аутентификация пользователей, в том числе:
* однократная аутентификация дает преимущество пользователям ЕСИАиА: пройдя процедуру идентификации и аутентификации в ЕСИАиА, пользователь может в течение одного сеанса работы обращаться к любым ИС, использующим ЕСИАиА, при этом повторная идентификация и аутентификация не требуется.
* Поддержка различных методов аутентификации по паролю и/или по электронной подписи;
* Поддержка уровней достоверности идентификации;
* Управление идентификационными данными.
* ведение регистров физических, юридических лиц, органов и организаций, должностных лиц органов и организаций и ИС;
* авторизация уполномоченных лиц МО при доступе к следующим функциям ЕСИАиА:
* ведение регистра должностных лиц МО в ЕСИАиА;
* ведение справочника полномочий ИС и предоставление пользователям ЕСИАиА (зарегистрированным в ЕСИАиА как должностные лица МО, ОУЗ) полномочий по доступу к ресурсам ИС, зарегистрированным ЕСИАиА;
* делегирование вышеуказанных полномочий уполномоченным лицам нижестоящих МО;
* ведение и предоставление информации о полномочиях пользователей в отношении информационных систем.

Для взаимодействия Системы в части обмена данными с внешними ИС должны быть разработаны форматы обмена данными в виде xml-шаблонов. Обмен данными должен происходить путем формирования xml-файла с необходимыми данными, передачи его во внешнюю ИС (или наоборот из внешней ИС в Систему) с последующим разбором файла и загрузкой данных в хранилище данных.

Система должна обеспечивать возможность информационного взаимодействия с внешними ИС на основе веб-сервисов, а также возможность расширения и внесения изменений в порядок и форматы этого взаимодействия без необходимости смены технологической платформы.

Для обмена информацией с другими системами должна использоваться технология SOAP (от англ. Simple Object Access Protocol, простой протокол доступа к объектам) — протокол, позволяющий передавать XML-форматированные сообщения посредством HTTP.

Система должна предоставлять программный интерфейс (Web API) для возможности осуществления идентификации и аутентификации пользователей ЕГИСЗ в федеральных и региональных прикладных системах ЕГИСЗ (приложениях ЕГИСЗ) через ЕСИАиА.

Обмен данными с ЕСИАиА должен осуществляться в соответствии с описанием протоколов взаимодействия данной Системы.

#### Система интеграции прикладных систем (ИПС)

Целью создания сервиса ИПС является автоматизация процессов информационного обмена между компонентами ЕГИСЗ и ведения баз метаданных об используемых сервисах участников предоставления услуг в сфере здравоохранения и фармакологии.

Система должна обеспечивать информационное взаимодействие прикладных подсистем федерального сегмента (ИАС УР, ЕСИАиА, ИЭМК, АХД и ФЭР) между собой, взаимодействие с внешними информационными системами и информационными системами Инфраструктуры электронного правительства (ЕПГУ, ЕСИА, СМЭВ) и единую точку входа для прикладных компонентов регионального сегмента при обращении к функциям прикладных компонентов федерального сегмента с использованием сервисно-ориентированной архитектуры (SOA) и технологии веб-сервисов.



Рисунок 5 - Структура системы ИПС

Для взаимодействия Системы в части обмена данными с внешними ИС должны быть разработаны форматы обмена данными в виде xml-шаблонов. Обмен данными должен происходить путем формирования xml-файла с необходимыми данными, передачи его во внешнюю ИС (или наоборот из внешней ИС в Систему) с последующим разбором файла и загрузкой данных в хранилище данных.

Для обмена информацией с другими системами должна использоваться технология SOAP (от англ. Simple Object Access Protocol, простой протокол доступа к объектам) — протокол, позволяющий передавать XML-форматированные сообщения посредством HTTP(S).

#### Система ведения нормативно-справочной информации (Система НСИ)

Система НСИ является информационным ядром управления ЕГИСЗ. Система НСИ обеспечивает согласованность и консолидацию данных, устраняет избыточность информации и оптимизирует поиск нужных сведений. Кроме того, справочники, входящие в НСИ, объединяют все остальные документы системы на протяжении всего их жизненного цикла.

Данный компонент разрабатывается для следующих целей:

* обеспечение учета, систематизации и управления нормативно-справочной информацией, применяемой в сфере здравоохранения;
* организация упорядоченного хранения и предоставление единой точки доступа к НСИ организациям сферы здравоохранения и внешним организациям;
* мониторинг и управление НСИ;
* обеспечение возможности использования данных НСИ при формировании форм учетно-отчетной документации;
* прием, учет и хранение данных НСИ от организаций, ответственных за ведение НСИ;
* обеспечение поддержки версионности обрабатываемой НСИ;
* организация централизованного хранения НСИ;
* обеспечение информационной безопасности;
* обеспечение учета ресурсов системы здравоохранения (федеральный регистр медицинского персонала, регистр паспортов медицинских учреждений, регистр оборудования).

### Принципы интеграции компонентов ЕГИСЗ с внешними информационными системами

Для взаимодействия Системы в части обмена данными с внешними ИС должны быть разработаны форматы обмена данными в виде xml-шаблонов и единая интеграционная шина для обеспечения единых форматов и регламентов взаимодействия с региональными ИС. Обмен данными должен происходить путем формирования xml-файла с необходимыми реквизитами, передачи его во внешнюю ИС (или наоборот из внешней ИС в Системы) с последующим разбором файла и загрузкой данных в хранилище данных.

Интеграция сервисов прежде всего необходима для создания единого информационного пространства с непротиворечивыми и объективными данными, исключающими необходимость двойного ввода информации.

Информационный обмен при развитии ЕГИСЗ будет построен с использованием общего интеграционного сервиса, который обеспечит интеграционное взаимодействие через единую точку входа информации с возможностью распределения нагрузки и мониторинга. Интеграционный сервис строится с учетом распределенной реализации компонент ЕГИСЗ.

Интеграционный сервис – это механизм для осуществления информационного взаимодействия системных компонентов, определенного правилами, соответствие которым является обязательным условием для включения информационных систем в состав ЕГИСЗ. Данные правила в качестве технических условий предъявляются к подключаемым в информационное взаимодействие системам.

Интеграция строится на основе общепринятых принципов взаимодействия информационных систем, протоколов и профилей.

Интеграционный сервис должен обеспечивать информационное взаимодействие прикладных систем федерального сегмента между собой, их взаимодействие с внешними информационными системами и информационными системами инфраструктуры Электронного правительства, а также должен представлять собой единую точку входа для прикладных компонентов регионального сегмента при обращении к функциям прикладных компонентов федерального сегмента с использованием сервисно-ориентированной архитектуры (SOA) и технологии веб-сервисов. Веб-сервисы описываются стандартным языком WDSL.

### Базовые требования к взаимодействию с внешними информационными системами

Система должна быть разработана с учетом возможности дальнейшей интеграции с Системой межведомственного электронного взаимодействия (СМЭВ). Для этого система должна удовлетворять требованиям, изложенными в приказе Минкомсвязи России от 27 декабря 2010 г. № 190 «Об утверждении Технических требований к взаимодействию информационных систем в единой системе межведомственного электронного взаимодействия».

Для интеграции со СМЭВ система должна удовлетворять следующим требованиям:

* требованиям к протоколам сетевого взаимодействия;

При использовании сетевых протоколов передачи данных необходимо придерживаться следующих спецификаций:

* протокол передачи гипертекста HTTP v. 1.1 – стандарт RFC 2616 инженерной группы проектировщиков информационно-телекоммуникационной сети Интернет (Internet Engineering Task Force, IETF);
* модернизированный протокол http v. 1.1 с обеспечением безопасности транспортного уровня (TLS) для существующего протокола управления передачей (TCP);
* протокол защищённых соединений SSL v. 3 / TLS – стандарт RFC 2246 инженерной группы проектировщиков информационно-телекоммуникационной сети Интернет (Internet Engineering Task Force, IETF);
* сервисы поддержки пространства имен DNS (Domain Name Services) – стандарт RFC 1035 инженерной группы проектировщиков информационно-телекоммуникационной сети Интернет (Internet Engineering Task Force, IETF).
* требованиям к протоколам веб-сервисов;

При разработке веб-сервисов необходимо придерживаться следующих спецификаций:

* базовый профиль интероперабельности v. 1.1 – стандарт Организации по интероперабельности веб-сервисов (Web Services Interoperability Organization Basic Profile 1.1, http://www.ws-i.org/Profiles/BasicProfile-1.1-2006-04-10.html) – спецификация носит обязательный характер;
* профиль передачи веб-сервисами бинарных приложений (WS-I Attachments Profile 1.0) – стандарт Организации по интероперабельности веб-сервисов WS-I (http://www.ws-i.org/Profiles/SimpleSoapBindingProfile-1.0.html http://www.ws-i.org/Profiles/AttachmentsProfile-1.0.html) – спецификация носит рекомендательный характер;
* профиль передачи веб-сервисами бинарных приложений (SOAP Message Transmission Optimization Mechanism) – стандарт консорциума W3C (http://www.w3.org/TR/soap12-mtom/) – спецификация носит рекомендательный характер;
* профиль связывания веб-сервисов (WS-I Simple SOAP Binding Profile 1.0) – стандарт организации по интероперабельности веб-сервисов WS-I (http://www.ws-i.org/Profiles/SimpleSoapBindingProfile-1.0.html, http://www.ws-i.org/Profiles/SimpleSoapBindingProfile-1.0.html) – спецификация носит рекомендательный характер;
* протокол SOAP 1.1 – стандарт консорциума W3C (http://www.w3.org/TR/soap/) – спецификация носит обязательный характер;
* язык описания веб-сервисов (Web Services Description Language, WSDL 1.1) – стандарт консорциума W3C (http://www.ws-i.org/Profiles/SimpleSoapBindingProfile-1.0.html, http://www.w3.org/TR/wsdl) – спецификация носит обязательный характер;
* политика использования веб-сервисов (Web Services Policy 1.2) – проект рекомендации консорциума W3C (http://www.ws-i.org/Profiles/SimpleSoapBindingProfile-1.0.htmlhttp://www.w3.org/Submission/WS-Policy/) – спецификация носит рекомендательный характер;
* спецификация универсального описания, обнаружения и интеграции веб-сервисов UDDI v. 3.0 (Universal Description Discovery and Integration) – стандарт Организации по развитию стандартов структурированной информации (Organization for the Advancement of Structured Information Standards, OASIS, http://www.uddi.org/specification.htm) – спецификация носит рекомендательный характер;
* спецификация универсального описания, обнаружения и интеграции веб-сервисов UDDI v. 2.0 (Universal Description Discovery and Integration) – стандарт Организации по развитию стандартов структурированной информации (Organization for the Advancement of Structured Information Standards, OASIS, http://www.uddi.org/specification.htm) – спецификация носит рекомендательный характер.
* требованиям к описанию данных;

При описании данных, метаданных и используемых наборов символов, применяемых в процессе информационного обмена, необходимо придерживаться следующих спецификаций:

* расширяемый язык разметки XML (Extensible Markup Language) – в соответствии с набором стандартов консорциума W3C (http://www.w3.org/XML);
* XML-схема (XML Schema 1.1, также допускается использование XMLSchema 1.0) – стандарты консорциума W3C, специфицированные в документах:
* XML-схемы Часть 1: Структуры (http://www.w3.org/TR/xmlschema-1/structures),
* XML-схемы Часть 2: Типы данных (http://www.w3.org/TR/xmlschema-2/datatypes);
* расширяемый язык таблиц стилей XSL v. 1.1 (Extensible Stylesheet Language) – стандарт консорциума W3C (http://www.w3.org/TR/xsl) определяющий XSL-преобразование (XSL Transformation) спецификацией (http://www.w3.org/TR/xslt).
* требованиям для подключаемых веб-сервисов;

При разработке веб-сервисов должны быть выполнены следующие особые условия и ограничения:

* согласно спецификации WS-I Basic Profile 1.1 все WSDL и XSD файлы должны быть кодированы в кодировке UTF-8 или UTF-16 (с указанием этой кодировки в заголовке XML);
* в WSDL описании веб-сервиса запрещены двунаправленные циклические ссылки из файла WSDL(1) на файл WSDL(2), если одновременно при этом файл WSDL(2) содержит ссылку на файл WSDL(1), несмотря на то, что спецификация WSDL 1.1 это допускает. Однонаправленные ссылки между файлами WSDL и XSD допустимы в любом количестве и сочетании;
* веб-сервис считается доступным только при одновременной доступности и точки доступа (endpoint) веб-сервиса и WSDL-писания веб-сервиса. Если не доступна точка доступа (endpoint) веб-сервиса, не должно быть доступно и WSDL-описание веб-сервиса, и, наоборот, если недоступно WSDL-описание веб-сервиса, то не должна быть доступна точка доступа (endpoint) веб-сервиса. Доступность веб-сервиса обеспечивает Поставщик веб-сервиса.
* необходимость использования encoding типа Document/Literal
* требованиям к обработке сообщений интерфейсом ИС, подключенной к системе взаимодействия;
* входящие сообщения, полученные по каналам связи системы взаимодействия, проходят контроль в следующем порядке:

проверка ЭЦП сообщения (включает в себя проверку всего набора данных входящих в сообщение - в том числе присоединенным к нему вложенных документов – файлов);

формально-логическая проверка сообщения.

* проверка ЭЦП сообщения осуществляется информационной системой, подключенной к системе взаимодействия, через подсистему проверки ЭЦП с использованием соответствующего удостоверяющего центра:

Выполняется проверка сертификата ЭЦП сообщения, в процессе которой устанавливается УЦ выдавший его. Производится определение легитимности данного УЦ с использованием сервисов ЕСИА, обеспечивающей интеграцию УЦ в рамках ЕПД.

После успешной идентификации сертификата и его проверки, выполняется проверка значения хеша сообщения и самого значения подписи.

* сообщения, ЭЦП для которых подтверждена, подвергаются формально-логической проверке значений реквизитов сообщения, заключающейся в проверке валидности формата и служебной информации сообщения, необходимой для его доставки и маршрутизации в рамках среды СМЭВ.
* в случае не прохождения формально-логической проверки, электронное сообщение исключается из дальнейшей обработки, данный факт фиксируется и отправителю направляется служебное электронное сообщение, извещающее об отказе в приеме сообщения.
* в случае прохождения формально-логической проверки сообщения, отправителю (порталу или ИС ведомства) направляется служебное электронное сообщение, извещающее об успешном приеме сообщения информационной системы, подключенной к системе взаимодействия.
* если принятое и успешно прошедшее процедуры контроля электронное сообщение является сообщением запроса на предоставление электронной услуги, то ИС Поставщика разрешает использование данного веб-сервиса.
* если принятое и успешно прошедшее процедуры контроля электронное сообщение является извещением о готовности данных, то ИС Получателя при необходимости инициирует сервис запроса этих данных.
* требованиям к структуре сообщений;

Требования к общей структуре SOAP-сообщения:

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

Тело сообщения должно в обязательном порядке содержать ряд служебных тегов. Веб-сервисы подключаемых ИС должны корректно обрабатывать и изменять информацию, содержащуюся в них.

* требованиям к документированию элементов метаданных;

Все элементы метаданных в XML-схеме должны быть документированы на русском языке.

Документирование элементов метаданных рекомендуется выполнять с использованием конструкции XMLSchema:

* <xsd:annotation>;
* <xsd:documentation>Текст описания</xsd:documentation>;
* </xsd:annotation>.

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

В качестве базового протокола сетевого и межсетевого взаимодействия должен использоваться TCP/IP (сокращение от английского Transfer Control Protocol/Internet Protocol, протокол управления передачей/интернет-протокол) – стек протоколов Интернета.

Вся информация, передаваемая по сети Интернет между компонентами Системы, должна шифроваться алгоритмами шифрования согласно ГОСТ 28147-89.

Доступ пользователей к интерфейсу Системы должен осуществляться по протоколу HTTPS (сокращение от английского – HyperText Transfer Protocol Secure – расширение протокола HTTP, поддерживающее шифрование).

Для взаимодействия Системы в части обмена данными с внешними ИС должны быть разработаны форматы обмена данными в виде xml-шаблонов. Обмен данными должен происходить путем формирования xml-файла с необходимыми данными, передачи его во внешнюю ИС (или наоборот из внешней ИС в Систему) с последующим разбором файла и загрузкой данных в хранилище данных.

Для обмена информацией с другими системами должна использоваться технология SOAP (от англ. Simple Object Access Protocol, простой протокол доступа к объектам) — протокол, позволяющий передавать XML-форматированные сообщения посредством HTTP(S).

Для стандартизации обмена медицинской информацией должны быть разработаны интеграционные профили, задающие сочетание и детализацию базовых национальных и международных стандартов информатизации здоровья, в частности HL7 v2.5, ISO/HL7 27931:2009 с использованием формата обмена сообщениями на основе XML (ANSI/HL7 V2 XML, R2-2012) и релевантных стандартов информационных и коммуникационных технологий.

Для обмена медицинской документацией с федеральным уровнем спецификации и технические условия обмена сведениями с федеральным сервисом Система ведения ИЭМК должны соответствовать следующим профилям Integrating the Healthcare Enterprise (IHE) с использованием стандартов HL7 CDA R2 или HL7 v2.5, внедренным на этапе разработки Системы ведения ИЭМК:

* IHE IT Infrastructure Technical Framework - Cross-Enterprise Document Sharing-b (XDS.b) – профиль поддержки публикации, хранения и доступа к СЭМД, включая поддержку транзакций:
* запись документа (ITI-42);
* получение документов (ITI-43).
* Basic Patient Privacy Consents (BPPC) – профиль поддержки политики конфиденциальности и обеспечения согласия пациента на публикацию его данных;
* IHE Audit Trail and Node Authentication (ATNA) – профиль поддержки аудита и аутентификации узла, включая:
* хранение данных об аудите;
* запись аудита (ITI-20);
* аутентификацию узла (ITI-19);
* поддержку единого времени в системе (ITI-1).
* требованиям к типам информационных потоков

Входная информация от внешних ИС должна подразделяться на следующие типы:

* управляющая информация информационного обмена (запросы, подтверждения);
* нормативно справочная информация в установленном правилами информационного обмена виде;
* медицинские документы, в установленном правилами информационного обмена виде.

Выходная информация из Системы во внешние ИС подразделяется на:

* управляющая информация информационного обмена (запросы, подтверждения);
* нормативно справочная информация в установленном правилами информационного обмена виде;
* информация для ведения медицинской статистики, аналитики, отчетности;
* медицинские документы, в установленном правилами информационного обмена виде.

## Технические требования к информационным системам ландшафта ФС ЕГИСЗ

При проектировании и разработке компонентов ФС ЕГИСЗ должны быть заложены основы для их дальнейшего развития и масштабирования.

Под масштабированием подразумевается увеличение количества обрабатываемой информации и количества пользователей.

Под развитием понимается создание новых программных средств на основе уже имеющихся с целью удовлетворения потребностей пользователей ФС ЕГИСЗ.

Модернизируемый ландшафт рассчитан на ежедневное непрерывное использование, что диктует повышенные требования к платформам, на которых они реализовываются. При разработке сервисов должны применяться исключительно промышленные платформы, которые зарекомендовали себя для использования в нагруженных распределенных системах с повышенными требованиями к отказоустойчивости и безопасности:

* программный код должен быть открытым и допускать его изменение;
* возможности программного средства должны быть достаточно подробно документированы;
* наличие успешных применений программного средства в законченных решениях;
* поддержка (использование) программного решения достаточным числом разработчиков;
* кроссплатформеность программного средства;
* способность программного средства работать с большими объемами информации.

При модернизации ландшафта необходимо учитывать уже используемые платформы и системные компоненты, развивать системы на базе уже имеющихся, сохраняя внедренный функционал и минимизируя количество используемых платформ для уменьшения стоимости сопровождения.

Проектируя ландшафт ФС ЕГИСЗ, требуется учитывать необходимость его масштабирования и увеличения нагрузки, а также необходимость расширять функционал. Любое масштабирование должно происходить без изменения бизнес-процессов и простоев системы более времени, указанного в соглашении об уровне сервиса.

Все сервисы должны быть разработаны с поддержкой аппаратной и программной масштабируемости и включать средства настройки, мониторинга и журналирования информационного взаимодействия.

В основу проектирования сервисов должен быть положен принцип максимально возможной централизации доступа к сервисам с учетом распределенного характера взаимодействия в рамках предоставления услуг в сфере здравоохранения и фармакологии.

Хранение данных в Системе должно быть обеспечено на основе современных реляционных или объектно-реляционных СУБД. Для обеспечения целостности данных должны использоваться встроенные механизмы СУБД.

Средства СУБД, а также средства используемых операционных систем должны обеспечивать протоколирование обрабатываемой в Системе информации.

Структура базы данных должна поддерживать хранение и обработку информации в соответствии с общероссийскими и отраслевыми классификаторами (там, где они применимы).

### Требования к масштабируемости ФС ЕГИСЗ

Система должна обладать свойствами приспособляемости и масштабируемости, заключающимися в возможности сохранения или повышении производительности при изменении условий эксплуатации, гибкости по отношению к изменениям, не связанным с коренным изменением нормативных документов, регулирующих деятельность пользователей Системы.

Требования к приспособляемости Системы заключаются в обеспечении возможности ее работоспособности в следующих случаях:

* при изменении количества потребителей информации;
* при изменении количества автоматизируемых функций;
* при изменении требований к безопасности Системы;
* при изменении количества поставщиков информации.

Изменение количества потребителей информации изменяет нагрузку на Веб-серверы (серверы приложений) Системы, что может вызвать необходимость повышения способности поддерживать увеличившееся количество одновременных обращений пользователей без существенной потери производительности и отказов в обслуживании обращений (нагрузочной способности) серверов. Увеличение нагрузочной способности может выполняться как за счет увеличения мощности веб-серверов (серверов приложений) Системы (увеличение количества процессоров либо модернизация до более производительных процессоров, увеличение объема оперативной памяти и дискового пространства), так и за счет увеличения количества серверов. При этом необходимо соблюдать следующие требования:

Системы должна адаптироваться к увеличению количества потребителей информации без необходимости изменения архитектуры Системы (сохранении принципов архитектуры DNA или установки дополнительного ПО);

Добавление новых серверов в состав группы Веб-серверов (серверов приложений) Системы не должно приводить к полной остановке функционирования Системы.

* Процедура публикации документов должна оставаться независимой от количества авторов;
* Безопасность Системы не должна ухудшаться при увеличении числа авторов;
* Механизмы подготовки и публикации документов должны обеспечивать возможность обслуживания всех авторов без снижения производительности;
* Должна быть обеспечена непрерывность процесса подготовки и публикации документов, насколько это возможно.

### Требования к расширению функциональных возможностей ФС ЕГИСЗ

Изменение количества функций, автоматизируемых с помощью систем, влечет изменение в программных модулях систем и их количестве, что влияет на нагрузку на серверы баз данных и веб-серверы (серверы приложений) систем. Увеличение нагрузки на серверы баз данных и веб-серверы (серверы приложений) Системы потребует повышения нагрузочной способности серверов. Увеличение нагрузочной способности может выполняться как за счет увеличения мощности серверов баз данных и веб-серверов (серверов приложений), так и за счет увеличения их количества. Также в этом случае может применяться технология объединения серверов баз данных в кластеры (кластерная технология), при которой несколько серверов вместе обрабатывают одни и те же операции (транзакции), распределяя нагрузку между собой (между узлами кластера). При этом необходимо соблюдать следующие требования:

* Система должна адаптироваться к повышению нагрузки на серверы баз данных и веб-серверы (серверы приложений), вызванной увеличением количества автоматизируемых пользовательских функций, без необходимости изменения архитектуры Системы (сохранении принципов архитектуры DNA или установки дополнительного ПО).
* Добавление новых серверов в состав группы серверов баз данных и/или веб-серверов (серверов приложений), а также применение технологии объединения серверов баз данных в кластеры, не должно приводить к полной остановке функционирования Системы.
* Система должна предусматривать возможность трехкратного масштабирования по производительности без модификации ее ПО, путем модернизации (расширения аппаратных ресурсов или замены на более производительные аппаратные компоненты) используемого комплекса технических средств или путем использования параллельной обработки части процессов (транзакций) на объединенных однотипных технических средствах. Возможности масштабирования должны обеспечиваться средствами используемого базового ПО.
* Серверные компоненты информационных систем ФС ЕГИСЗ размещаются и функционируют в ФЦОД Заказчика, реализуя все функциональные возможности и обеспечивая их предоставление в виде информационно-коммуникационных технологических услуг на АРМ пользователей и персонала.

Технические требования к серверным мощностям должны рассчитываться исходя из показателей назначения.

В соответствии с концепцией ФС ЕГИСЗ ФЦОД является ее основным элементом инфраструктуры. Для обеспечения требуемого уровня показателей надежности и доступности информационно-технических сервисов количество территориально удаленных площадок, на которых размещается ФЦОД, может изменяться по мере развития ФС ЕГИСЗ.

Основная площадка и площадка «горячего» резерва ФЦОД могут функционировать в режиме разделения нагрузки и оперативного перераспределения выполняемых функций в случае отказов оборудования и систем на одной из этих площадок. Площадка «холодного» резерва предназначена для резервирования основной площадки и площадки «горячего» резерва ФЦОД на случай стихийных бедствий и других событий катастрофического характера, при которых функционирование площадок полностью или в значительной степени нарушено. Площадки ФЦОД связаны между собой высокоскоростной и высоконадежной сетью передачи данных.

Инфраструктура Системы удовлетворяет следующим требованиям:

* соответствие используемых технических решений масштабам бизнес-задач, бизнес-целям и бизнес-стратегиям объектов автоматизации;
* унификация и типизация компонентов инфраструктуры для снижения совокупной стоимости владения;
* структуризация инфраструктуры с выделением ЦОД различного уровня для повышения эффективности, надежности, отказоустойчивости и безопасности используемых информационных ресурсов;
* соответствие международным и российским ИТ-стандартам, а также лучшей мировой практике построения ИТ-инфраструктуры.

C учетом перспективы развития ФС ЕГИСЗ необходимо обеспечить проектирование компонент на основе модели их размещения как на федеральном уровне, так и на региональных узлах федерального ЦОД.

### Требования к изменению уровня безопасности Системы

Изменение требований к безопасности Системы оказывает влияние на все его составные части. Система должна адаптироваться в соответствии с изменяющимися требованиями с соблюдением следующих условий:

* в процессе адаптации защищенность не должна становиться хуже существующей на момент начала адаптации;
* процесс адаптации не должен прерывать доступа потребителей информации к информационным ресурсам;
* процесс адаптации не должен прерывать процесс подготовки и публикации документов;
* процесс адаптации не должен затрагивать тех пользователей, на которых не распространяются новые требования.

Все технические решения, использованные при разработке компонентов Системы, а также требования к аппаратному обеспечению, должны соответствовать действующим нормам и требованиям законодательства в области безопасности и защиты персональных данных, в том числе нормативным правовым и организационно распорядительным документам по технической защите информации, принятым ФСТЭК и ФСБ России.

### Требования к защите информации от несанкционированного доступа

Компоненты ФС ЕГИСЗ должны быть защищены от угроз, возникающих в процессе их функционирования, в частности:

* обход злоумышленником защитных средств;
* переход сервиса в небезопасное состояние в результате сбоя или отказа, при начальной загрузке, в процессе или после перезагрузки;
* маскарад пользователя (попытка злоумышленника выдать себя за уполномоченного пользователя, в частности, за администратора). В распределенной среде маскарад может реализовываться путем подмены исходного адреса или воспроизведения ранее перехваченных данных идентификации/аутентификации;
* использование злоумышленником чужого сетевого соединения или интерактивного сеанса (например, путем доступа к оставленному без присмотра терминалу);
* несанкционированное изменение злоумышленником конфигурации прикладного ПО и/или конфигурационных данных;
* несанкционированный доступ к конфиденциальной (например, регистрационной) информации, в том числе несанкционированное расшифровывание зашифрованных данных;
* несанкционированное изменение данных (например, регистрационной информации), в том числе таких, целостность которых защищена криптографическими методами.

В рамках требований к защите информации должны быть обеспечены следующие возможности:

* реализация аутентификации пользователей с использованием интерфейса пользователя, предоставляемого сервером ЕСИАиА для идентификации и аутентификации через логин и пароль условно-постоянного действия или с использованием электронной подписи;
* реализация возможности применения механизмов мандатного принципа доступа;
* реализация механизма блокировки входа при заданном количестве неудачных попыток ввода идентификатора и пароля;
* реализация возможности отнесения каждого пользователя – сотрудника МО к одной из двух категорий, отличающихся правами доступа к информационным объектам:
* категория обычных (рядовых) пользователей – штатные сотрудники учреждений, потребители и провайдеры информации;
* категория привилегированных пользователей – сотрудники отдела эксплуатации МО, а также представители организации-разработчика изделия (либо уполномоченных специалистов других организаций, имеющих партнерские отношения с организацией-разработчиком).
* пользователи должны быть зарегистрированы в ЕСИАиА на индивидуальной основе;
* пользователи должны быть отнесены к одной или нескольким ролевым группам;
* электронное взаимодействие между системами в рамках ФС ЕГИСЗ должно осуществляться на основе сертификатов (ключей, токенов);
* ни одна из описанных функций прикладных компонент ФС ЕГИСЗ не должна быть доступна никому из пользователей системы, если это не задано явно администратором системы, который имеет абсолютные полномочия;
* интерфейс администрирования должен позволять задавать перечень функций из числа описанных, доступных конкретному пользователю;
* должна иметься возможность определения перечня функций для создаваемой администратором системы группы пользователей;
* должна быть обеспечена функция регистрации и учета событий (журналирование), обеспечивающая:
* регистрацию входа/выхода пользователей в систему и из системы;
* регистрацию результата попытки входа: успешная или неуспешная, несанкционированная, идентификатор субъекта, предъявленный при попытке доступа (имя пользователя):
* при вводе в процессе аутентификации неправильного сочетания имя пользователя/пароль фиксацию в системном журнале времени неудачной попытки входа, предъявленного имени пользователя и имени домена для входа;
* регистрацию в системном журнале время выхода, имя пользователя, управляющая сведениями о пользователе система, идентификатор входа и тип входа при выходе пользователя из системы;
* регистрацию доступа к контролируемым приложениям;
* регистрацию события подготовки документов для печати и/или отправки документов на печать.
* должна быть обеспечена функция контроля целостности, обеспечивающая:
* периодическое тестирование целостности компонент (системных файлов) в процессе функционирования системы;
* возможность экспорта/импорта настроек для быстрого восстановления системы в случае сбоев или отказов системы.

Общую структуру Системы следует классифицировать как специализированную многопользовательскую среду, в которой различные категории пользователей имеют различные права доступа к информации.

Система должны обеспечить следующие возможности:

* уникальность идентификаторов и паролей пользователей;
* фиксацию в электронном журнале событий, связанных с выполнением операций, инициируемых действиями пользователей;
* просмотр и анализ электронного журнала зафиксированных событий.

Безопасность информации в системе должна обеспечиваться за счет согласованного применения технологических, организационных, технических и программных мер и средств защиты на всех этапах подготовки, обработки, передачи и хранения информации:

* на системном уровне;
* на уровне сервера баз данных;
* на прикладном уровне.

Должна быть обеспечена возможность защиты конфиденциальной информации, в т.ч. за счет использования технологий псевдонимизации структурированных персональных медицинских данных, содержащихся в составе ИЭМК, на основе международного стандарта ISO/TS 25237:2008 «Health informatics – Pseudonymization».

Должна быть обеспечена возможность использования электронной подписи в процессе обмена СЭМД между Системой и внешними системами.

Передача данных между Системой и внешними системами должна осуществляться по защищённым каналам связи.

### Перечень аварийных ситуаций

Ниже приводится перечень возможных аварийных ситуаций с указанием требований к средствам восстановления работоспособности Системы:

* Сбой общего или специального программного обеспечения Системы (отдельного АРМ, веб-сервера (сервера приложений) или сервера баз данных). После сбоя операционной системы веб-сервера (сервера приложений) или сервера баз данных, или СУБД в процессе выполнения пользовательских задач должно быть обеспечено восстановление данных в базе данных до состояния на момент окончания последней нормально завершенной перед сбоем операции (транзакции). Время восстановления работоспособности при сбоях и отказах не должно превышать 3-х часов. В это время не входит разворачивание и настройка специального программного обеспечения Системы на веб-сервере(ах) (сервере(ах) приложений) и сервере(ах) баз данных. В указанное время не входит решение проблем с техническим обеспечением и инсталляцией операционных систем указанных серверов.
* Выход из строя части технических средств Системы. Выход из строя одного из АРМ или нарушение канала связи локальной сети между АРМ и веб-сервером (сервером приложений) не должны приводить к прекращению функционирования Системы, при этом должна обеспечиваться возможность выполнения функций, связанных с вышедшим из строя АРМ, на другом АРМ.
* Сбои или выход из строя активного накопителя на жестком магнитном диске. Система должна обеспечивать возможность «горячей» замены активного накопителя на жестком магнитном диске без остановки функционирования Системы и потерь информации. В Системе должна быть обеспечена возможность восстановления данных с внешнего накопителя после восстановления активного накопителя.
* Импульсные помехи, сбои или прекращение электропитания. Импульсные помехи, сбои или прекращение электропитания не должны приводить к выходу из строя технических средств Системы и/или нарушению целостности данных в БД Системы. Прекращение электропитания на время, регламентированное нормативными документами МЗ, до 15 минут не должно приводить к прекращению функционирования Системы. Должны быть предусмотрены средства оповещения пользователей о прекращении электропитания.

### Требования к надежности технических средств и программного обеспечения ФС ЕГИСЗ

Надежность Системы в части технического обеспечения должна обеспечиваться:

* использованием технических средств повышенной отказоустойчивости и их структурным резервированием;
* наличием на объектах автоматизации запасных изделий и приборов (далее - ЗИП);
* защитой технических средств по электропитанию путем использования источников бесперебойного питания;
* дублированием носителей информационных массивов.

Компоненты ФС ЕГИСЗ должны обеспечивать корректную обработку ошибочных ситуаций с возможностью дальнейшего продолжения работы без аварийного закрытия подсистем, за исключением случаев, когда ошибка делает дальнейшую работу в рамках пользовательской сессии невозможной. Надежность специального прикладного ПО должна быть обеспечена комплексом мероприятий отладки, поиска и исключения ошибок на этапах доработки функциональной архитектуры и приемо-сдаточных испытаний.

Программное обеспечение не должно реагировать непредсказуемым образом на штатные действия администраторов и/или пользователей.

Ввод данных недопустимого типа не должен приводить к аварийным ситуациям.

Система должна обеспечивать возможность восстановления работы программного обеспечения средствами системы резервного копирования.

Система должна эксплуатироваться в круглосуточном режиме с учетом технологических профилактических перерывов и перерывов на проведение регламентных работ. Длительность перерывов не должна превышать времени, принятого в соглашении об уровне сервиса.

Оценка надежности должна осуществляться на всех стадиях разработки посредством анализа полноты архитектурных и технических решений по построению Системы и их соответствия техническим требованиям настоящего документа.

## Описание технических требованиям к информационным сервисам в рамках развития компонентов ФС ЕГИСЗ

При осуществлении развития компонентов ФС ЕГИСЗ необходимо учитывать требования программных платформ, тип и версию программного обеспечения, использованное для создания сервисов на предыдущих этапах. Модернизировать информационные системы следует сохраняя уже используемый функционал и отдавая преимущество уже используемому программному обеспечению.

### Технические требования к развитию сервиса ФЭР

Для создания всех функциональных подсистем федеральной электронной регистратуры должно использоваться свободно распространяемое ПО (в качестве серверной операционной системы Linux (например, Ubuntu Server 11.10), в качестве сервера приложений JBoss версии 5.1.0, в качестве СУБД PostgreSQL.

Проектирование модели предметной области (бизнес-процессов) ФЭР должно осуществляться с использованием нотации BPMN (системы условных обозначений (нотации) для моделирования бизнес-процессов).

Проектирование структур баз данных должно выполняться с использованием нотации UML или IDEF1X.

### Технические требования к развитию сервиса ИАС УР

При разработке ИАС УР использованы следующие платформы и сторонние библиотеки:

* PHP 5.2.3;
* jQuery;
* PL\SQL;
* xml.

На серверах баз данных ИАС УР установлены следующие компоненты, расширяющие возможности операционной системы:

* СУБД ORACLE 10g Database Server.

На веб-серверах ИАС УР установлены следующие компоненты, расширяющие возможности ИАС УР:

* IIS 6.0;
* PHP 5.2.3;
* АК «ПРОГНОЗ»;
* ORACLE 10g x32 InstantClient.

Проектирование структуры центрального хранилища данных Системы выполнено с использованием средства ErWin на основе реляционного подхода. Создание и управление ЦХД Системы осуществляется средствами ORACLE 10g Database Server.

Для обеспечения возможности реализации системы бизнес-анализа показателей назначения должно использоваться свободно распространяемое ПО, например, Pentaho 5.0.

### Технические требования к развитию Системы НСИ

Проектирование структуры базы данных Системы НСИ выполнено с использованием средства ErWin на основе реляционного подхода.

Создание и управление базы данных Реестра НСИ осуществляется средствами ORACLE 10g Database Server.

При разработке Системы НСИ использованы следующие платформы и сторонние библиотеки:

* PHP;
* PEAR;
* jQuery;
* PL\SQL;
* АК «ПРОГНОЗ».

В состав программного обеспечения Системы НСИ не входят средства, расширяющие возможности операционной системы.

### Технические требования к развитию сервиса ИЭМК

Проектирование модели предметной области (бизнес-процессов) ИЭМК должно осуществляться с использованием BPMN (системы условных обозначений (нотации) для моделирования бизнес-процессов).

Проектирование структур баз данных должно выполняться с использованием нотации UML или IDEF1X.

В процессе разработки должна использоваться современная система контроля версий, например, Subversion (SVN).

При разработке ИЭМК должны использоваться следующие технологии:

* основной язык разработки - Java;
* основная технология - JavaEE 5;
* для доступа к данным должен использоваться протокол JDBC;
* общие сервисные компоненты должны быть реализованы с помощью технологий Spring;
* в качестве сервера приложений должен использоваться сервер приложений с открытым исходным кодом, например Glassfish v2.

### Технические требования к функционированию РИП ММД

На федеральном уровне функциональные модули размещаются на ФЦОД с их обязательным дублированием на резервной площадке и включают в себя:

* центральный сервер РИП ММД, полностью поддерживающий стандарт DICOM 3.х в кластерном исполнении;
* интеграционный модуль РИП ММД, предназначенный для интеграции со сторонними системами;
* модуль, обеспечивающий web-доступ к исследованиям;
* модуль диагностической рабочей станции врача с функцией записи на CD-диск.

Федеральная инфраструктура РИП ММД должна поддерживать базовые интеграционные профили IHE (XDS, ATNA, PIX, PDQ), а также специализированные профили IHE, имеющие отношение к работе с медицинскими изображениями и данными электронной медицинской карты.