УТВЕРЖДЕНО

приказом ГБУ СО «РЦУП»

от «22» апреля 2011 г. № 242-ссн

ИНТЕГРАЦИОННАЯ ШИНА ЭЛЕКТРОННОГО ПРАВИТЕЛЬСТВА САМАРСКОЙ ОБЛАСТИ

СПЕЦИФИКАЦИЯ ТРЕБОВАНИЙ К ПРОТОТИПУ ИНФОРМАЦИОННОЙ СИСТЕМЫ ИШ ЭП СО

ЛИСТОВ 59

Самара 2011 г.

ЛИСТ СОГЛАСОВАНИЯ

Спецификация требований к прототипу информационной системы ИШ ЭП СО

ГБУ СО РЦУП

Должность	ФИО	Подпись	Дата
Заместитель директора	Д.П.Шевченко		15.04.2011
Начальник управления по развитию и сопровождению информационных систем и ресурсов	А.В.Ягупов		17.04.2011
Главный инженер проекта	С.А.Кузьминов		8.04.2011
Главный инженер проекта	Н.В.Кутузов		08.04.2011

Содержание

Введение

Данный документ описывает требования, предъявляемые к прототипу информационной системы Интеграционная шина электронного правительства Самарской области. Для данной информационной системы в документе допускается использование следующих обозначений – «Прототип», «ИШ ЭП СО».

В рамках данного документа применяются следующие понятия:

- Услуга — нормативно закрепленная услуга, которая оказывается органами исполнительной власти гражданам, бизнесу или другим государственным структурам.
- Электронная услуга (далее – ЭУ) – услуга, оказываемая с помощью информационно-коммуникационных технологий. С технической точки зрения процесс оказания ЭУ начинается с формирования запроса на системе-потребителе и заканчивается предоставлением ответа системы-провайдера. Под ответом здесь понимается результат оказания ЭУ (предоставление информации, предоставление документа, изменение статуса получателя услуги).
- Регламент оказания ЭУ – свод процедурных правил, устанавливающих порядок оказания ЭУ.
- Система-участник – любая информационная система, участвующая в процессе информационного взаимодействия, проходящего с использованием ИШ ЭП СО. Система-участник может быть либо системой потребителем, либо системой-провайдером.
- Система-потребитель – информационная система, заинтересованная в получении результатов оказания электронной услуги. Для получения результатов формируется запрос установленной структуры (требования к структуре запроса описываются в

документе требований к услуге, который формируется в каждом конкретном случае);

- Система-провайдер – информационная система, предоставляющая результат оказания услуги (или часть результата в случае композитных услуг). Результат формируется в виде ответа установленной структуры (требования к структуре ответа описываются в документе требований к услуге, который формируется в каждом конкретном случае).
- Сообщение – XML-файл установленной структуры [**Ошибка! Источник ссылки не найден.**], используемый в процессе информационного взаимодействия, проходящего с использованием ИШ ЭП СО. Существуют следующие типы сообщений:
    - Запрос – сообщение, формируемое системой-потребителем и содержащее данные, необходимые для получения ЭУ.
    - Ответ – сообщение, формируемое системой-провайдером в ответ на запрос и содержащее данные результата оказания ЭУ.
- Системное сообщение-отказ – сообщение, формируемое ИШ ЭП СО в результате наступления исключительных ситуаций (предупреждения, ошибки, сбои).
- Синхронный тип взаимодействия – тип информационного взаимодействия, при котором управление системе-потребителю возвращается только после полного завершения процесса обработки запроса и предоставления ответа. Для получения ответа не требуется осуществление дополнительных взаимодействий с системой-провайдером. При этом типе взаимодействия ответ на запрос представляется в течение фиксированного периода времени, не превышающего стандартное время ожидания (90 секунд).

- Асинхронный тип взаимодействия – тип информационного взаимодействия, при котором управление системе-потребителю возвращается до истечения времени, необходимого на обработку запроса и предоставление ответа. При этом типе взаимодействия для получения ответа требуется осуществлять дополнительные взаимодействия с системой-провайдером (получение статуса предоставления ЭУ, получение ответа).

1. Общие требования к прототипу

Прототип должен обеспечивать поддержку стандарта обмена сообщениями SOAP 1.1, желательна поддержка SOAP 1.2.

Прототип должен обеспечивать следующие возможности:

- управление потоком и маршрутизацией сообщения;
- публикация сторонних web-сервисов;
- обращение к сторонним web-сервисам;
- интеграцию с UDDI реестром сервисов;
- параллельную обработку сообщений;
- слияние и разделение потоков сообщений;

Прототип должен обеспечивать реализацию различных моделей взаимодействий:

- request/reply (запрос/ответ);
- point-to-point (точка-точка);
- publish/subscribe (публикация/подписка);
- multicast (многоадресная рассылка).

Прототип должен обеспечивать расширенную поддержку веб-сервисов:

- SOAP/HTTP;
- SOAP/JMS;
- Web Services Description Language (WSDL);
- Web Services Gateway.

Прототип должен обеспечивать поддержку:

- WS-* Standarts (WS-Security, WS-Atomic Transactions, включая

UDDI Registry, для публикации и управления сервисами и метаописанием точек взаимодействия);

- селекторов, обеспечивающих динамический выбор и вызов различных сервисов, использующих один и тот же интерфейс;
- JCA адаптеров;
- механизмов состояний процесса и управляющих правил;
- использования в интеграционных взаимодействиях задач с участием человека;
- механизмов версионности интеграционных компонентов;
- синхронных и асинхронных способов информационного обмена;
- динамического изменения маршрутов и внутренней обработки сообщений;
- WSDL / XSD описаний сервисов;
- веб-сервисов нотификаций, публикации и подписки на нотификации;
- системы обработки исключительных ситуаций;
- автопроверки состояния сервисов;
- аудита событий.

Прототип должен обеспечивать реализацию:

- средств проверки работоспособности сервисов;
- механизмов управления транзакциями и безопасностью.

Прототип должен обеспечивать возможность:

- публикации адаптеров к внешним системам;
- реализации адаптеров к распространенным форматам сообщений;

- создания и использования механизма управления бизнес-процессами, совместимого со стандартом BPEL.

Прототип должен обеспечивать работу с доверенным сертифицированным удостоверяющим центром, обеспечивающим идентификацию, аутентификацию и авторизацию пользователей и систем-участников.

2. Функции системы

Прототип должен реализовывать следующие основные функции:

- транспортные:
    - маршрутизация сообщений;
    - доставка сообщений.
- прикладные:
    - предоставление интерфейса web-сервиса ЭУ;
    - реализация бизнес-логики осуществления ЭУ;
    - формирование запросов в систему-провайдер;
    - предоставление ответа системы-провайдера системе-потребителю;
    - форматно-логический контроль (далее – ФЛК) сообщений в контексте ЭУ.
- общесистемные:
    - аутентификация систем-потребителей;
    - авторизация систем-потребителей;
    - проверка сертификатов и ЭЦП систем-участников (контроль сообщений);
    - проверка сертификатов и ЭЦП пользователей;
    - формирование «жетона» (идентификатора сообщения);
    - преобразование форматов сообщений и интерфейсов взаимодействия;
    - формирование ЭЦП ИШ ЭП СО;
    - формирование и предоставление статуса оказания ЭУ;

- публикация и хранение web-сервисов;
- формирование системных сообщений-отказов для систем-участников;
- формирование задач с участием человека;
- предоставление и хранение общесистемной и общеупотребимой нормативно-справочной информации (далее – НСИ);
- журналирование действий ИШ ЭП СО;
- взаимодействие с доверенным удостоверяющим центром ЭП СО.

2.1. Требования к транспортным функциям

2.1.1. Требования к маршрутизации сообщений

Прототип должен поддерживать статическую и динамическую маршрутизацию сообщений.

Статическая маршрутизация должна производиться с помощью адреса получателя, жестко прописанного в интеграционных модулях.

Динамическая маршрутизация должна производиться с использованием адреса получателя, содержащегося в репозитории сервисов.

Динамическая маршрутизация должна производиться с учетом системной логики обработки сервисов. Прототип должен иметь возможность использования средств для конфигурирования системной логики обработки сервисов.

Средства маршрутизации должны обеспечивать доставку сообщений одному или нескольким получателям согласно системной логике обработки сервисов.

2.1.2. Требования к доставке сообщений

Прототип должен обеспечивать отправку запросов от системы-получателя к системе-провайдеру.

Прототип должен обеспечивать доставку ответов от системы-провайдера к системе-потребителю.

Прототип должен содержать настраиваемые механизмы повторной доставки сообщений в случае, если доставка с первого раза не удалась.

Прототип должен иметь возможность использовать для доставки сообщений механизмы гарантированной доставки сообщений.

2.2. Требования к прикладным функциям

2.2.1. Требования к предоставлению интерфейса web-сервиса ЭУ

Прототип должен предоставлять для системы-потребителя интерфейс для вызова web-сервиса соответствующей ЭУ.

Интерфейс должен содержать информацию об адресе размещения сервиса и наименование функции.

Требования к web-сервису (к интерфейсу, в том числе) разрабатываются в каждом конкретном случае и описываются в документе требований к соответствующей услуге.

Информация о web-сервисе ЭУ и метаданные web-сервиса ЭУ должны быть размещены в реестре и репозитории сервисов. Общие требования к web-сервисам приведены в спецификации требований к интерфейсам взаимодействия [**Ошибка! Источник ссылки не найден.**].

2.2.2. Требования к реализации бизнес-логики осуществления ЭУ

Прототип должен реализовывать бизнес-логику предоставления ЭУ в соответствии с логикой, описанной в документе требований к соответствующей услуге.

Прототип должен проводить следующие обязательные операции, не зависящие от бизнес-логики оказания ЭУ:

- журналирование событий (раздел 2.3.14);
- контроль сообщений (раздел 2.3.3);
- проверка сертификата и ЭЦП пользователя (раздел 2.3.4);
- ФЛК сообщений (раздел 2.2.5);
- формирование запроса в систему-провайдер (раздел 2.3.5)
- формирование жетона (только для асинхронных типов взаимодействия) (раздел 2.3.6);
- формирование ЭЦП ИШ ЭП СО (раздел 2.3.8);
- формирование статуса оказания ЭУ (раздел 2.3.9);
- предоставление ответа системы-провайдера.

2.2.3. Требования к формированию запроса в систему-провайдер

Прототип должен формировать запрос в систему-провайдер на основании данных, полученных от системы-потребителя, путем заполнения блока «системная информация». Блок «Системная информация» заполняется в соответствии с правилами заполнения [**Ошибка! Источник ссылки не найден.**].

2.2.4. Требования к предоставлению ответа

Ответ системы-провайдера должен помещаться в системное хранилище и сохраняться там до момента передачи ответа системе-потребителю.

Прототип должен предоставлять системе-потребителю ответ системы-провайдера на основании предъявленного жетона.

Предъявление жетона означает окончание процесса обработки данных на ИШ ЭП СО. При предъявлении жетона (окончании процесса обработки данных) ответ системы-провайдера должен быть передан системе-потребителю и удален из системного хранилища ИШ ЭП СО.

В прототипе должна быть реализована возможность удаления ответа из системного хранилища по истечении заданного срока, если за этот период времени не был предъявлен жетон. По умолчанию период хранения устанавливается равным 10 рабочим дням. Период хранения может быть изменен в соответствии с регламентными требованиями оказания ЭУ.

2.2.5. Требования к форматно-логическому контролю (ФЛК) сообщений

Прототип должен выполнять ФЛК получаемых сообщений на предмет корректности содержащихся данных. Основными правилами проведения ФЛК являются:

- соблюдение формата передаваемых данных;
- соблюдение обязательности заполнения полей, подлежащих обязательному заполнению, согласно контексту информационного взаимодействия;
- выполнение особых условий, накладываемых на передаваемые данные.

Подробные правила ФЛК сообщений указываются в документе требований к каждой конкретной электронной услуге, осуществляемой посредством ИШ ЭП СО.

Если условия ФЛК не выполняются, дальнейшая обработка сообщения прекращается. ИШ ЭП СО формирует и отправляет системное сообщение-отказ с указанием кода ошибки (см. раздел 2.3.11).

Допускается реализация ФЛК с использованием динамически подгружаемых модулей проверок или формализованных бизнес-правил.

2.3. Требования к общесистемным функциям

2.3.1. Требования к аутентификации систем-потребителей

Прототип должен проводить аутентификацию систем-потребителей на основании сертификата системы, выданного РУЦ.

Для проведения процесса аутентификации систем-потребителей должен быть создан реестр доверяемых систем. Реестр содержит данные сертификатов систем, которым разрешено обращение к ИШ ЭП СО.

Прототип должен иметь средства, позволяющие управлять реестром доверяемых систем.

В случае, если процесс аутентификации завершился с отрицательным результатом, формируется системное сообщение-отказ, содержащее код ошибки (см. раздел 2.3.11). Системное сообщение-отказ должно формироваться встроенными средствами интеграционной платформы ИШ ЭП СО.

2.3.2. Требования к авторизации систем-потребителей

Прототип должен проводить авторизацию систем-потребителей для получения прав доступа к сервисам ЭУ и сервисам получения НСИ на основании сертификата системы, выданного РУЦ.

Для проведения процесса авторизации для каждой системы-потребителя должны быть назначены права доступа к сервисам ЭУ и сервисам получения НСИ.

В случае, если процесс авторизации завершился с отрицательным результатом, формируется системное сообщение-отказ, содержащее код ошибки (см. раздел 2.3.11). Системное сообщение-отказ должно формироваться встроенными средствами интеграционной платформы ИШ ЭП СО.

2.3.3. Требования к проверке сертификата и ЭЦП системы-участника (контроль сообщений)

Прототип должен содержать механизмы, осуществляющие входной контроль получаемых сообщений (запросов и ответов) на основании ЭЦП сообщения, сформированного системой-участником.

Контроль выполняется по направлениям:

- проверка ЭЦП системы-участника;
- проверка сертификата открытого ключа системы-участника.

Контроль сообщений осуществляется в соответствии с рекомендациями WS security [**Ошибка! Источник ссылки не найден.**].

В случае если условия контроля не выполняются, формируется системное сообщение-отказ, содержащее код ошибки (см. раздел 2.3.11). Системное сообщение-отказ должно формироваться встроенными средствами программного обеспечения ИШ ЭП СО.

2.3.4. Требования к проверке сертификата и ЭЦП пользователя

Прототип должен содержать механизмы проверки действительности сертификата и ЭЦП пользователя, содержащихся в получаемых сообщениях.

Сертификат и ЭЦП пользователя должны быть проверены в соответствии с требованиями проверки сертификатов и ЭЦП [**Ошибка! Источник ссылки не найден.**].

Если условия проверки не выполняется, обработка сообщения прекращается. ИШ ЭП СО формирует отправителю сообщения системное сообщение-отказ с указанием кода ошибки (см. раздел 2.3.11).

2.3.5. Требования к формированию запроса в систему-провайдер

Прототип должен формировать запрос в систему-провайдер на основании данных, полученных от системы-потребителя, путем заполнения блока «системная информация». Блок «Системная информация» заполняется в соответствии с правилами заполнения [**Ошибка! Источник ссылки не найден.**].

2.3.6. Требования к формированию жетона

Прототип должен формировать жетон, который впоследствии позволяет однозначно идентифицировать сообщение.

Жетон содержит следующие атрибуты:

- GUID – идентификатор, используемый в процессе информационного машинного взаимодействия.
- Номер жетона – идентификатор, используемый при взаимодействии пользователя и системы-потребителя.

GUID должен формироваться стандартными средствами языка программирования в соответствии со спецификацией Microsoft (http://msdn.microsoft.com/en-us/library/aa373931(VS.85).aspx).

Номер жетона формируется в формате, адаптированном для восприятия пользователя: ДДММГГ-XXXXXX, где:

- ДДММГГ – дата подачи запроса;
- XXXXXX – целое число, формируемое инкрементным образом (+1). По окончании календарного дня значение обнуляется. Первое значение нового дня должно иметь значение 1 (единица).

2.3.7. Требования к преобразованию объектов и интерфейсов

Прототип должен содержать механизмы, позволяющие приводить формат передаваемых сообщений к формату, используемому системой-получателем. Требования к преобразованию объектов и форматов разрабатываются в каждом конкретном случае и описываются в документе требований к соответствующей услуге.

Прототип должен иметь возможность производить преобразование интерфейсов для различных систем посредством адаптеров. Требования к адаптерам разрабатываются в каждом конкретном случае и описываются в документе требований к соответствующей услуге.

2.3.8. Требования к формированию ЭЦП ИШ ЭП СО

Прототип должен подписывать передаваемые сообщения ЭЦП ИШ ЭП СО. При этом ЭЦП и сертификат открытого ключа записывается в SOAP заголовок сообщения.

Под ЭЦП ИШ ЭП СО понимается ЭЦП уполномоченного лица организации, ответственной за эксплуатацию ИШ ЭП СО. ЭЦП ИШ ЭП СО формируется с использованием цифрового сертификата, выданного РУЦ [**Ошибка! Источник ссылки не найден.**].

2.3.9. Требования к формированию и предоставлению статуса оказания ЭУ

Прототип должен обладать средствами для формирования и предоставления информации о статусе оказания ЭУ. Информация о статусе оказания ЭУ должна предоставляться по данным жетона.

Статус оказания ЭУ может принимать одно из следующих значений:

- запрос принят на обработку, статус присваивается в момент успешной передачи запроса от системы-потребителя к ИШ ЭП СО;
- запрос на обработке, статус присваивается в момент успешной

передачи запроса от ИШ ЭП СО в систему-провайдер;

- запрос обработан, статус присваивается в момент получения ИШ ЭП СО результата обработки запроса от системы-провайдера;
- запрос выполнен, статус присваивается, когда ответ системы-провайдера был передан в систему-потребитель и запрос был закрыт ввиду исполнения;
- ошибка при обработке запроса, статус присваивается в случае, если в результате выполнения запроса возникла ошибка и запрос не может быть исполнен;
- ответ удален по истечении срока хранения, статус присваивается, когда результат обработки удален принудительно – не последовало предъявление жетона в период, установленный в соответствии с регламентными требованиями оказания ЭУ.

Прототип должен обладать возможностью изменения списка обязательных статусов в зависимости от регламентных требований к оказанию ЭУ.

2.3.10. Требования к публикации и хранению web-сервисов

Прототип должен обеспечивать публикацию, хранение и управление web-сервисами посредством реестра и репозитория сервисов.

Реестр сервисов должен обеспечивать:

- регистрацию web-сервиса;
- поиск и предоставление информации о web-сервисе по заданным критериям поиска.

Реестр сервисов должен разрабатываться в соответствии со спецификацией UDDI.

Репозиторий сервисов должен обеспечивать:

- хранение web-сервисов и метаданных сервисов;
- доступ к web-сервисам и метаданным сервисов;
- добавление web-сервисов и метаданных сервисов;
- модификацию существующих web-сервисов и метаданных сервисов
- удаление web-сервисов и метаданных сервисов.

2.3.11. Требования к формированию системных сообщений-отказов для участников информационного взаимодействия

Прототип должен формировать системные сообщения-отказы для участников информационного взаимодействия в следующих исключительных ситуациях:

- сообщение не прошло контроль сообщения на ИШ ЭП СО:
    - ошибка в заголовке сообщения;
    - сертификат системы отсутствует в РУЦ;
    - сертификат системы недействителен;
    - неверный тип сертификата;
    - корневой сертификат не может быть получен;
    - неверный алгоритм ЭЦП;
    - ЭЦП системы недействительна;
    - сообщение утратило силу в связи истечением срока действия ЭЦП.
- система не прошла аутентификацию:
    - сертификат системы отсутствует в РУЦ;
    - сертификат системы недействителен;
    - система отсутствует в реестре доверенных систем.

- система не прошла авторизацию:
    - доступ к запрашиваемой услуге запрещен.
- сертификат пользователя недействителен:
    - сертификат пользователя отсутствует в РУЦ;
    - сертификат пользователя недействителен;
    - неверный тип сертификата;
    - корневой сертификат не может быть получен.
- ЭЦП пользователя недействительна:
    - неверный дескриптор провайдера или объекта хеширования;
    - неверный алгоритм ЭЦП;
    - открытый ключ подписи содержит дескриптор недопустимого открытого ключа;
    - ЭЦП пользователя неверна.
- сообщение не прошло ФЛК:
    - формат данных не соответствует требованиям;
    - обязательные поля не заполнены;
    - размерность полей не соответствует требованиям;
    - особые условия не выполнены.
- прочие ситуации, зависящие от бизнес-логики оказания ЭУ.

Системное сообщение-отказ должно направляться в систему, которая предоставила сообщение, вызвавшее одну или несколько исключительных ситуаций. Описание исключительной ситуации осуществляется посредством указания кода ошибки в блоке «Системная информация». Код ошибки указывается из справочника ответных сообщений, ошибок и исключительных ситуаций [**Ошибка! Источник ссылки не найден.**].

Системное сообщение-отказ в случае ситуаций «система не прошла аутентификацию», «система не прошла авторизацию» должно формироваться встроенными средствами интеграционной платформы ИШ ЭП СО.

Прототип должен обладать возможностью изменять перечень исключительных ситуаций, при которых формируется системное сообщение-отказ, в зависимости от конкретного перечня оказываемых ЭУ.

2.3.12. Требования к взаимодействию оператора и сервиса

Прототип должен обладать механизмом, который позволяет взаимодействовать оператору и сервису или части сервиса. Данный механизм обеспечивает реализацию сервисов ЭУ, где невозможно осуществить процесс без участия человека.

Механизм должен позволять назначать задачи или сервисы конкретному оператору или ролевой группе операторов.

Механизм должен реализовывать следующие типы задач с участием человека:

- запуск процесса – оператор инициализирует процесс или сервис;

- фрагмент процесса – оператор выполняет действия, являющиеся частью процесса или сервиса.

2.3.13. Требования к размещению, хранению и использованию НСИ

2.3.13.1. Общесистемные справочники

Прототип должен обеспечить хранение общесистемных справочников и классификаторов, необходимых для осуществления процессов информационного взаимодействия систем.

На прототипе должны быть реализованы web-сервисы, предназначенные для предоставления версий общесистемных справочников системе-потребителю.

Информация о web-сервисе предоставления общесистемных справочников и метаданные web-сервиса должны быть размещены в реестре и репозитории сервисов.

Описание общесистемных справочников и web-сервисов предоставления приведено в документе «Общесистемные справочники и классификаторы, хранимые в информационной системе ИШ ЭП СО».

2.3.13.2. НСИ систем-провайдеров

Прототип должен обеспечить хранение локальных версий справочников и классификаторов систем-провайдеров, используемых в процессе оказания ЭУ.

Прототип должен обеспечить регулярный опрос систем-провайдеров на предмет появления обновленных версий справочников и обновлять локальные справочники в случае наличия обновленной версии. Процесс опроса должен запускаться автоматически по заданному графику обновлений или с оговоренной периодичностью. Справочные данные должны храниться в БД и передаваться от систем-провайдеров в XML формате. Обновление справочников должно производиться с помощью web-сервисов.

На прототипе должны быть реализованы web-сервисы, предназначенные для предоставления системе-потребителю обновленных версий справочников системы-провайдера.

Информация о web-сервисе обновления справочников и метаданные web-сервиса обновления должны быть размещены в реестре и репозитории сервисов.

Информация о web-сервисе предоставления справочников и метаданные web-сервиса предоставления должны быть размещены в реестре и репозитории сервисов.

Требования к web-сервисам обновления и предоставления справочников систем-провайдеров разрабатываются в каждом конкретном случае и описываются в документе требований к соответствующей услуге.

2.3.14. Требования к журналированию работы

В целях мониторинга и осуществления аудита прототип должен обеспечить журналирование событий, связанных с работой ИШ ЭП СО.

Прототип должен обеспечить следующие уровни журналирования событий:

- Отладка (debug) – максимальный уровень журналирования;
- Ошибки (error) – уровень журналирования ошибок;

- Все (all) – уровень журналирования всех ошибок;
- Выключено (off) – уровень, при котором журналирование отключено;
- Критичные ошибки (fatal) – уровень журналирования только ошибок, приводящих к останову приложения;
- Диагностика (warn) – уровень журналирования диагностических сообщений;
- Аудит (audit) – уровень журналирования событий аналитического аудита.

Журналирование должно предусматривать фиксацию следующих видов событий:

- события аналитического аудита;
- системные события.

События аналитического аудита должны обеспечивать сохранение всей цепочки взаимодействия с ИШ ЭП СО, включая события перехода между состояниями процесса взаимодействия.

Журнал событий должен разделяться на две части:

- оперативный журнал аудита;
- архивный журнал событий.

В оперативном журнале аналитического аудита хранятся все события, сообщения-запросы и сообщения-ответы, которые относятся к ЭУ, оказываемым в данный момент. При предъявлении жетона или истечении срока предоставления ответа, происходит перемещение событий в архивный журнал событий. При этом все сообщения-запросы и сообщения-ответы, связанные с оказанием конкретной услуги уничтожаются. Таким образом, архивный журнал событий хранит факты совершения событий и результаты событий.

Результаты выполнения операций записываются в журнал событий в хронологическом порядке.

Записи в журнал событий подлежат события, указанные в таблице 1.

Таблица 1 – События, подлежащие журналированию

Событие	Уровень журналирования	Примечание
Получение запроса системы-потребителя	Audit	
Получение ответа системы-провайдера	Audit	
Формирование в прототипе запроса в систему-провайдер;	Audit	
Предоставление жетона системе-потребителю	Audit	только в случае асинхронного типа взаимодействия
Получение жетона от системы-потребителя для выдачи ответа	Audit	только в случае асинхронного типа взаимодействия

Событие	Уровень журналирования	Примечание
Отправка сообщения системе-провайдеру	Audit	
Преобразование интерфейса	Audit	
Получение обновления справочника от системы-провайдера	Audit	
Контроль сообщения	Audit	
Выполнение процесса проверки ЭЦП и сертификата системы	Audit	
Выполнение процесса проверки ЭЦП и сертификата пользователя	Audit	
Выполнение ФЛК входящих сообщений	Audit	
Выполнение процесса формирования жетона с указанием данных жетона	Audit	
Выполнение процесса подписания сообщений ЭЦП ИШ ЭП СО	Audit	
Сохранение ответа от системы-провайдера в системном хранилище	Audit	
Поиск ответа в системном хранилище	Audit	

Событие	Уровень журналирования	Примечание
Удаление ответа из системного хранилища	Audit	
Запрос информации о статусе оказания ЭУ	Audit	
Предоставление данных о статусе оказания ЭУ	Audit	

Журнал должен содержать следующие данные о произошедшем событии:

- дата и время события;
- наименование события.
- результат события – результат, с которым завершился процесс;
- компонент – наименование компонента, вызвавшего операцию журналирования;
- идентификатор – GUID сообщения (после формирования жетона), либо псевдоним системы (до момента формирования жетона);
- xml-файл запроса, ответа (в краткосрочном журнале аудита);
- дополнительная информация – указываются дополнительные сведения о результате выполнения.

Для фиксации ошибок и исключительных ситуаций необходимо журналировать следующие данные:

- Java класс события аудита;
- место выброса ошибки (модуль - функция - строка);

- примечание разработчика при обработке ошибки;
- фрагмент системного лога или xml файл сообщения;
- дата и время возникновения ошибки;
- пользователь, в сессии которого произошла ошибка;
- приоритет ошибки согласно уровням логирования log4j (DEBUG, INFO, WARN, ERROR, FATAL);
- событие аудита;
- экземпляр процесса.

Прототип должен обладать возможностью изменять перечень событий, подлежащих журналированию.

Журнал событий может представлять собой удобочитаемый текстовый файл, размещаемый в предопределенной директории, предназначенной для хранения логов, или схему базы данных. Доступ к директории для хранения логов или базе данных должен иметь только пользователь с правами администратора ИШ ЭП СО.

Для файла логов должен быть предусмотрен механизм формирования нового экземпляра журнала событий, при достижении им определенного размера. Предыдущие журналы событий должны архивироваться с указанием в имени файла диапазона дат тех событий, информацию о которых они содержат.

Доступ к механизмам журналирования должен быть разрешен пользователям, обладающим правами администратора ИШ ЭП СО.

2.3.15. Требования к взаимодействию с доверенным удостоверяющим центром

Прототип должен обладать функциональностью для взаимодействия с доверенным удостоверяющим центром ЭП СО.

Прототип должен взаимодействовать с РУЦ при установлении факта действительности цифровых сертификатов открытых ключей, выданных пользователям и системам-участникам информационного взаимодействия в рамках ЭП СО.

Прототип должен обладать средствами для получения с сервера РУЦ списка отозванных сертификатов (CRL).

Прототип должен обладать возможностью осуществлять взаимодействие с РУЦ по протоколу OCSP.

2.4. Требования к взаимодействию модулей в рамках функционирования информационной системы ИШ ЭП СО

Исходя из функций, описанных в разделе 1, прототип функционально состоит из следующих модулей:

- сервис предоставления услуги;
- диспетчер сообщений;
- сервис преобразования объектов и интерфейсов;
- реестр и репозиторий сервисов;
- модуль контроля сообщений;
- модуль аутентификации и авторизации;
- модуль ФЛК;
- модуль ЭЦП;
- модуль формирования жетонов;

- системное хранилище;
- хранилище НСИ;
- модуль журналирования.

Сервис предоставления услуги является механизмом, реализующим процесс предоставления ЭУ, и обладает следующей функциональностью:

- предоставление интерфейса web-сервиса ЭУ для системы-потребителя;
- формирование запроса в систему-провайдер;
- реализация бизнес-логики предоставления ЭУ;
- выдача ответа системе-потребителю.

Диспетчер сообщений предназначен для выполнения следующих задач:

- маршрутизация сообщений;
- доставка сообщений.

Сервисы преобразования объектов и интерфейсов осуществляют преобразование сообщений (запросов и ответов) в формат, с которым работает соответствующая система-участник.

Реестр и репозиторий сервисов является хранилищем интерфейсов веб-сервисов и форматов данных.

Модуль контроля сообщений выполняет функцию контроля сообщений.

Модуль аутентификации и авторизации осуществляет аутентификацию и авторизацию систем-потребителей;

Модуль ФЛК выполняет функции форматно-логического контроля;

Модуль ЭЦП предназначен для выполнения следующих задач:

- проверка сертификатов и ЭЦП пользователей;
- формирование ЭЦП ИШ ЭП СО.

Модуль формирования жетонов реализует функцию формированию жетона;

Системное хранилище предназначено для оперативного хранения ответов систем-провайдеров;

Хранилище НСИ выполняет функции по хранению и управлению НСИ;

Модуль журналирования осуществляет журналирование событий, возникших в процессе работы ИШ ЭП СО.

Схема, описывающая взаимодействие модулей при оказании ЭУ, представлена на рисунке 1.

Процесс взаимодействия выполняется следующим образом.

1. Из системы-потребителя в ИШ ЭП СО поступает запрос на оказание электронной услуги. Факт получения запроса фиксируется в журнале событий.
2. Модуль контроля сообщений ИШ ЭП СО выполняет проверку полученного сообщения: действительность сертификата и ЭЦП системы-потребителя.
    a. Если сертификат и ЭЦП запроса действительны, запрос поступает на дальнейшую обработку. Результат успешной проверки ЭЦП фиксируется в журнале событий.
    b. Если сертификат и ЭЦП запроса недействительны, процесс дальнейшей обработки прекращается. В этом случае:
        i. Формируется запись в журнале событий о наличии запроса с недействительной ЭЦП и причинами отказа от дальнейшей обработки.

ii. На ИШ ЭП СО формируется отказ с указанием кода ошибки.

iii. Отказ передается в систему-потребитель.

3. Компонент аутентификации и авторизации ИШ ЭП СО выполняет проверку системы, посредством которой произошло обращение за услугой:

   a. Если результат аутентификации и авторизации положительный, осуществляется дальнейшая обработка запроса. Факт аутентификации и авторизации фиксируется в журнале событий.

   b. Если результат аутентификации или авторизации отрицательный, обработка запроса прекращается. В этом случае:

      i. Формируется запись в журнале событий о неуспешной авторизации и аутентификации.

      ii. ИШ ЭП СО формирует отказ с указанием кода ошибки.

      iii. Отказ передается в систему-потребитель.

4. Происходит вызов сервиса предоставления ЭУ, запрос поступает в данный сервис. Запускается механизм, обеспечивающий бизнес-логику оказания ЭУ.

5. Сервис предоставления услуги вызывает модуль проверки ЭЦП. Выполняются проверка сертификата и ЭЦП пользователя, который обратился за услугой.

   a. Если проверка выполнена успешно (сертификат и ЭЦП действительны), обработка запроса продолжается. В журнале событий фиксируется факт проверки запроса.

b. Если проверка выполнена неуспешно (сертификат пользователя или ЭЦП недействительны), обработка запроса прекращается. В этом случае:

   i. В журнале событий фиксируется запись об отрицательном результате проверки сертификата или ЭЦП пользователя.

   ii. ИШ ЭП СО формирует отказ с указанием кода ошибки.

   iii. Отказ передается в систему-потребитель.

6. Сервис предоставления услуги вызывает модуль ФЛК. Выполняется форматно-логический контроль сообщения.

   a. Если результат ФЛК положительный, обработка запроса продолжается. В журнале событий фиксируется факт прохождения сообщением ФЛК.

   b. Если сообщение не прошло ФЛК, обработка запроса прекращается. Далее:

      i. В журнале событий фиксируется отказ от дальнейшей обработки сообщения с указанием причины и результатами ФЛК.

      ii. ИШ ЭП СО формирует отказ с указанием кода ошибки.

      iii. Отказ передается в систему-потребитель.

7. Сервис предоставления услуги запускает процедуру формирования жетона. Формируется жетон с указанием номера и GUID сообщения для последующей уникальной идентификации запроса. Информация о жетоне записывается в журнал событий.

8. Сервис предоставления услуги передает сформированный жетон в систему-потребитель.

9. При необходимости преобразования запроса в формат системы-провайдера, сервис предоставления услуги передает запрос в сервис преобразования объектов и интерфейсов. Выполняется преобразование запроса в формат системы-провайдера. Результат фиксируется в журнале событий.
10. Сервис предоставления услуги передает сообщение на подписание ЭЦП. Запрос подписывается, при этом факт подписи запроса отражается в журнале событий.
11. Запрос передается в диспетчер сообщений.
12. Диспетчер сообщений запрашивает адрес сервиса системы-провайдера в репозитории сервисов.
13. Репозиторий сервисов возвращает ответ с указанием адреса web-сервиса системы-провайдера.
14. Диспетчер сообщений вызывает сервис системы-провайдера и передает запрос. Результат фиксируется в журнале событий.
15. Диспетчер сообщений получает ответ от системы-провайдера в виде сообщения, записывает факт получения в журнал событий.
16. При необходимости преобразования ответа в формат системы-получателя, диспетчер сообщений передает запрос в сервис преобразования объектов и интерфейсов. Выполняется преобразование ответа в формат системы-получателя. Результат фиксируется в журнале событий.
17. Модуль контроля сообщений ИШ ЭП СО выполняет контроль полученного сообщения.

a. Если контроль пройден, то сообщение-ответ сохраняется в хранилище. Результат контроля сообщения фиксируется в журнале событий. Факт помещения ответа в системное хранилище фиксируется в журнале событий.

b. Если контроль не пройден, процесс дальнейшей обработки прекращается. В этом случае:

   i. Формируется запись в журнале событий о наличии ответа с недействительным сертификатом или ЭЦП, а также с причинами отказа от дальнейшей обработки.

   ii. На ИШ ЭП СО формируется отказ с указанием кода ошибки.

   iii. Отказ передается системе-провайдеру.

18. Сервис предоставления услуги ожидает запрос (жетон) от системы-получателя для получения результата оказания услуги.

19. Сервис предоставления услуги получает жетон от системы-получателя для предъявления результатов оказания электронной услуги. Факт получения жетона записывается в журнал событий.

20. По данным жетона выполняется поиск ответа в системном хранилище.

a. Если ответ по данным жетона найден, ответ извлекается и передается на дальнейшую обработку. Положительный результат поиска ответа фиксируется в журнале.

b. Если ответ по данным жетона не найден, передача ответа по результату оказания электронной услуги невозможна. В данном случае:

i. В журнале событий указывается отрицательный результат поиска ответа по жетону.

ii. На ИШ ЭП СО формируется отказ от предоставления ответа с указанием кода ошибки.

iii. Отказ передается в систему-потребитель.

21. Извлеченный из хранилища ответ передается в модуль ЭЦП и подписывается ЭЦП ИШ ЭП СО. Факт подписи фиксируется в журнале событий.

22. Сервис предоставления услуги передает подписанный ответ в систему-потребитель.

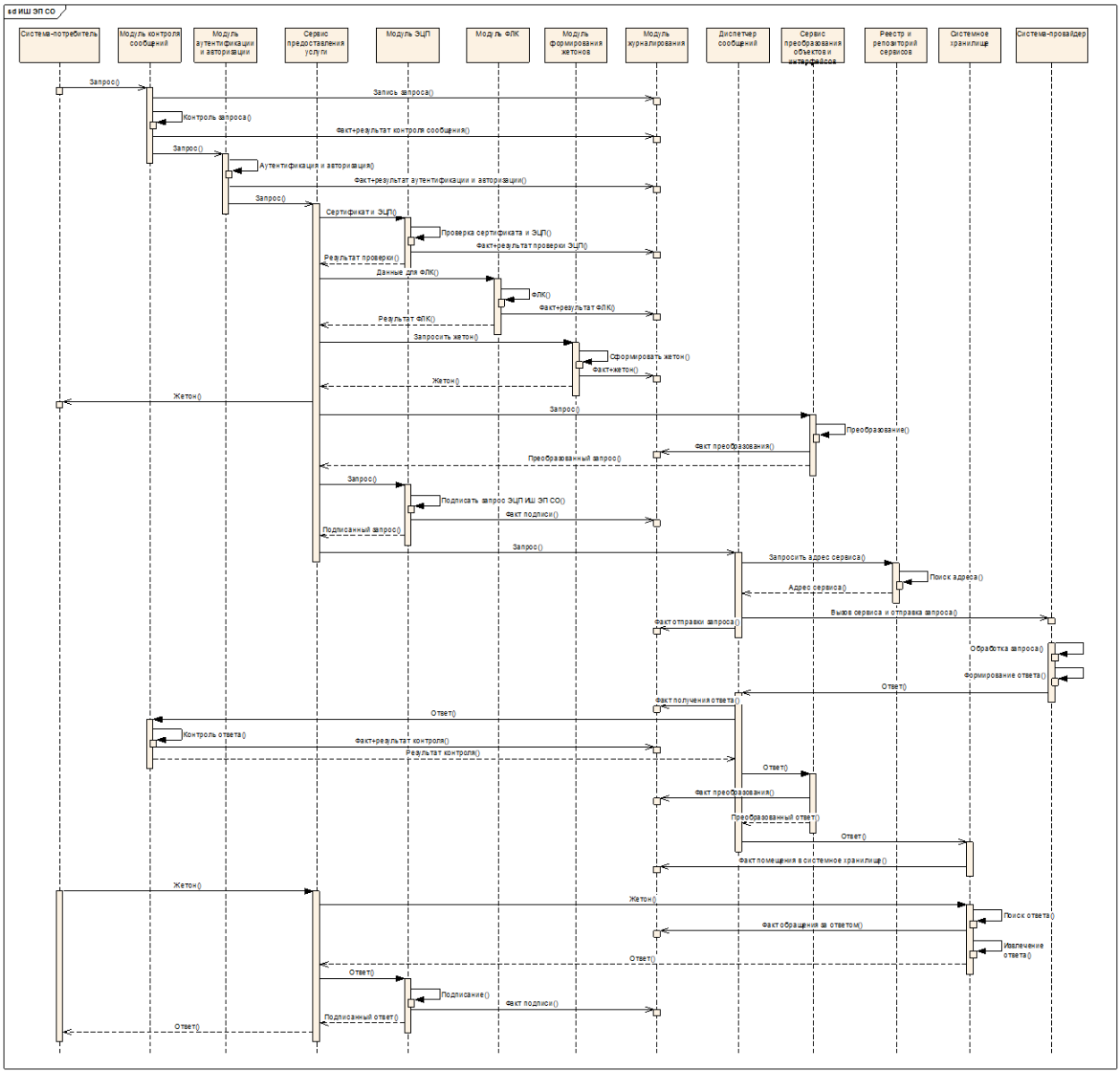

Рисунок 1 – Взаимодействие модулей ИШ ЭП СО

3. Требования к аппаратному обеспечению

При выборе технических средств, обеспечивающих функционирование системы, целесообразно исходить из следующих общих требований:

- производители и поставщики технических средств и решений должны иметь апробированные продукты и обеспечивать надежные гарантии;
- техническое обеспечение должно обеспечивать решение всех возложенных на систему задач и обеспечивать определенный запас «мощности» на случай быстрого роста потребностей;
- техническое обеспечение должно обеспечивать преемственность по отношению к существующим техническим решениям;
- комплекс решений должен представлять собой законченный программно-технический продукт, допускающий тиражирование, что позволяет минимизировать затраты на проектирование, ввод в эксплуатацию и сопровождение системы;
- техническое обеспечение должно быть инвестиционно защищенным, т.е. технические средства должны быть масштабируемыми по производительности, емкости оперативной памяти, емкости дискового пространства и числу каналов ввода-вывода, а поставщики оборудования - иметь долгосрочные программы поддержки этих устройств.

3.1. Требования к аппаратному обеспечению серверов

Требования к серверному оборудованию, необходимому для функционирования ИШ ЭП СО, указаны в таблице 2.

Таблица 2 – Характеристики необходимого серверного оборудования

№	Оборудование	Техническая характеристика	Кол-во, шт.
Интеграционная шина			
1	Процессор	Intel Xeon® Dual-Core (3.0 GHz)	2
	Оперативная память	от 8 Gb (PC2-5300 Fully Buffered DIMMs DDR2-667)	
	Дисковый массив	от 40 Gb (Hot Plug SAS/SATA HDD)	
БД интеграционной шины			
2	Процессор	Intel Xeon® Quad-Core (1.8 GHz)	1
	Оперативная память	от 8 Gb (PC2-5300 Fully Buffered DIMMs DDR2-667)	
	Дисковый массив	от 2 Tb (Hot Plug SAS/SATA HDD)	

3.2. Требования к активному и пассивному сетевому оборудованию

Активное сетевое оборудование системы должно использовать:

- отказоустойчивую архитектуру;
- технологии коммутации интерфейсов Ethernet при построении локальных вычислительных сетей (далее – ЛВС);
- оборудование и решения, обеспечивающие масштабируемость ЛВС без необходимости замены оборудования.

Активное сетевое оборудование системы, реализующее функции основной транспортной магистрали, должно иметь модульную архитектуру и поддерживать отказоустойчивые конфигурации за счет:

- дублирования блоков питания;
- дублирования модулей управления и маршрутизирующих модулей;
- поддержки технологий резервирования каналов.

Активное сетевое оборудование системы должно обеспечивать поддержку технологий Fast Ethernet и/или Gigabit Ethernet.

Для построения ЛВС прототипа должно использоваться оборудование, обеспечивающее организацию магистрали с пропускной способностью не менее 100 Мбит/с.

Кабельная система должна включать кабельную магистраль и кроссовые соединения в распределительных узлах. Кабельная система должна выполняться на кабеле "витая пара" и коммутационных элементах не ниже 5-й категории для обеспечения передачи данных со скоростью до 100 Мбит/с. Для обеспечения более высоких скоростей передачи данных кабельная система должна выполняться на многомодовом оптоволоконном кабеле.

Кабельные соединения должны обеспечивать подключение необходимого количества активных сетевых устройств в каждом распределительном узле. Должно быть предусмотрено резервирование кабельных соединений, предназначенное для развития и модернизации сети, а также для использования в случаях возможных отказов в основных кабельных соединениях.

3.3. Мониторинг и управление

Необходимо обеспечить мониторинг и управление сетевыми, вычислительными и информационными ресурсами, включая комплекс технических средств системы. Комплекс мер по обеспечению мониторинга и управления должен охватывать:

- инвентарный контроль и управление изменениями в информационной системе;
- контроль и централизованное распространение программного обеспечения;
- удаленное управление программным обеспечением комплекса технических (аппаратно-программных) средств;
- мониторинг состояния технических средств;
- мониторинг и управление активным сетевым оборудованием;
- сбор и анализ статистики, отчетность и поддержка принятия решений по обслуживанию программного обеспечения и комплекса технических средств системы, в том числе для активного управления, т.е. выявление возможных проблем на ранней стадии и недопущение возникновения критических ситуаций.

Мониторинг и управление техническими средствами должен обеспечивать выполнение следующих функций:

- управление всеми типами устройств в сети, поддерживающих SNMP протокол;
- мониторинг состояния устройств и их интерфейсов;
- графическое представление физических устройств и связей в сети;
- графическое или иное удобное для восприятия представление логической структуры сети, включая существующие виртуальные сети;
- графическое представление устройств с возможностью управления отдельными модулями и/или интерфейсами;
- разграничение полномочий управления отдельными устройствами и

группами устройств в сети;

- сбор и анализ результатов мониторинга устройств с использованием графического интерфейса и различных форм представления полученных данных, в том числе для активного управления.

3.4. Выделенная электрическая сеть

Выделенная электрическая сеть (ВЭС) должна быть выполнена в соответствии с требованиями построения, определенными в стандартах и правилах ПУЭ (Правила устройства электроустановок) издание 6-е, 1998 г., ГОСТ 12.1.030-81.

ВЭС здания должна обеспечивать подключение оконечного оборудования, а также его перемещение внутри здания без перестройки электрической сети (т.е. без перепрокладки трасс).

Кабельные трассы должны выдерживать на любых участках двукратную пиковую нагрузку по току.

Прием и распределение электроэнергии по потребителям в помещениях здания должны осуществляться следующим образом:

- в здании должен быть установлен распределительный щит системы гарантированного электропитания (ЩР СГЭ);
- ЩР СГЭ должен быть подключен через защитные автоматы к главному распределительному щиту или входному распределительному устройству здания;
- от ЩР СГЭ должна быть выполнена кабельная разводка ВЭС до мест размещения потребителей;
- все розетки, установленные на месте размещения потребителей, должны подключаться к защитным автоматам в ЩР СГЭ.

ЩР СГЭ должен быть подключен к общему контуру заземления здания.

Все компоненты ВЭС должны быть унифицированы. Вся электрическая разводка должна выполняться проводом, обеспечивающим заземление потребителей.

Все активные устройства в шкафах должны быть заземлены путем подключения к заземленному проводу однофазной трехпроводной сети электропитания. Заземление корпусов распределительных узлов через заземляющий зажим корпуса должно осуществляться от ближайшего распределительного щита медным изолированным проводником («земля»). Сечение защитного проводника выбирается согласно требованиям ГОСТ Р 50571.10-96.

Пересечение кабелей ЛВС и ВЭС должно выполняться под прямым углом.

Должна быть обеспечена защита помещений, в которых расположены серверы, от электромагнитного излучения силовых электроустановок, расположенных в соседних помещениях (лифты и пр.).

4. Требования к программному обеспечению

Перечень серверного ПО для функционирования ИШ ЭП СО, приведен в таблице 3.

Таблица 3 – Перечень серверного ПО для функционирования ИШ ЭП СО

№ п/п	Наименование ПО	Описание	Количество лицензий, шт.
1	IBM Web Sphere Process Server 6.1	Сервер интеграции бизнес процессов (основа создание SOA, WS-BPEL).	2
2	Oracle Database Enterprise Edition10g	СУБД	1
3	Red Hat Enterprise Linux 5	Серверная операционная система	3

5. Требования к обеспечению ИБ

Применяемые для обеспечения информационной безопасности средства и технологии защиты должны удовлетворять требованиям Концепции информационной безопасности правительства Самарской области и технической политике, проводимой Правительством Самарской области.

Применяемые средства и технологии защиты должны обеспечивать необходимую и достаточную защиту информационных ресурсов от угроз безопасности, определенных моделью угроз безопасности информационным ресурсам Правительства Самарской области.

Применяемые средства и технологии защиты должны обладать свойствами модульности и масштабируемости.

Для эффективной эксплуатации и сопровождения системы обеспечения информационной безопасности должен быть предусмотрен комплекс организационно-технических мер и разработаны необходимые организационно-распорядительные документы.

5.1. Требования к защите от несанкционированного доступа к защищаемой информации

ИШ ЭП СО должна проводить аутентификацию сторон-участников информационного взаимодействия с использованием цифровых сертификатов формата X.509v3, выданных РУЦ. Для проведения процесса аутентификации должен быть создан реестр доверяемых систем, содержащий данные сертификатов систем, которым разрешено обращение к ИШ ЭП СО.

Для всех сторон-участников, а также операторов ИШ ЭП СО должно проводиться разграничение доступа к сервисам и средствам администрирования ИШ ЭП СО. В ИШ ЭП СО должны быть реализованы средства эффективного управления и контроля предоставления прав доступа.

Должен быть разработан набор регламентной документации, определяющий порядок доступа к сервисам ИШ ЭП СО. Доступные права доступа, роли и их комбинации должны быть описаны в рабочей документации.

Для компонентов технической инфраструктуры ИШ ЭП СО должен быть организован процесс регулярной установки обновлений.

Компоненты технической инфраструктуры ИШ ЭП СО должны располагаться в рамках защищенной сетевой инфраструктуры, построенной на основе виртуальной частной сети VipNet. Для предотвращения несанкционированного доступа к информации в процессе передачи по каналам связи должно использоваться шифрование каналов с использованием алгоритмов, соответствующих российским стандартам.

Для предотвращения несанкционированного физического доступа к компонентам технической инфраструктуры ИШ ЭП СО должна быть введена разграничительная система доступа и использоваться инженерно-технические системы защиты.

5.2. Требования к средствам обеспечения целостности и достоверности защищаемых данных

В ИШ ЭП СО должны быть реализованы средства, позволяющие использовать ЭЦП для подписи сообщений и проверки подписи в соответствии с требованиями документа «Спецификация требований к механизмам постановки и проверки ЭЦП» и WSS: SOAP Message Security 1.1 (WS-Security 2004).

Для всех компонентов технической инфраструктуры ИШ ЭП СО должна быть организована антивирусная защита.

5.3. Требования по использованию ЭЦП

В ИШ ЭП СО должны использоваться средства работы с ЭЦП, соответствующей ГОСТ 34.10-2001.

В ИШ ЭП СО должны быть реализованы программные средства, обеспечивающие идентификацию подписи, проверку цепочки сертификатов, а также проверку статусов сертификатов в цепочке.

ИШ ЭП СО должна взаимодействовать с РУЦ при проверке статусов сертификатов систем-участников информационного взаимодействия.

Ключи ЭЦП, используемые в процессе информационного взаимодействия, должны быть созданы с применением сертифицированных средств.

Должна быть организована система доверия между сертификатами пользователей, выданными разными УЦ.

5.4. Требования к подсистеме аудита

В целях мониторинга и осуществления аудита ИШ ЭП СО должна обеспечить журналирование событий, связанных с работой ИШ ЭП СО. Журналы аудита должны быть защищены от несанкционированного доступа.

На компонентах технической инфраструктуры ИШ ЭП СО должны быть установлены агенты подсистемы аудита, позволяющие производить регистрацию критических системных событий и событий безопасности.

Подсистема аудита должна позволять проводить настройку списка контролируемых событий.

5.5. Требования к подсистеме хранения защищаемой информации

Должна быть организована защита от несанкционированного копирования информации из подсистемы хранения.

В подсистеме хранения должно проводиться резервное копирование информации, обеспечивающее возможность её оперативного восстановления. Резервные копии должны регулярно тестироваться.

6. Требования к размещению

Информационная система ИШ ЭП СО должна размещаться на серверных площадках, входящих в состав аппаратно-программного комплекса Правительства Самарской области или организациях, ему подведомственных.

Аппаратно-программный комплекс должен размещаться в помещениях, подконтрольных Правительству Самарской области. Доступ в помещения должен регламентироваться действующими требованиями по обеспечению безопасности.

Серверные приложения подлежат размещению на 3-х выделенных серверах – два сервера приложений и сервер БД. Серверы приложений программно объединяются в кластер для распределения нагрузки и повышения скорости обработки запросов.

Основная установка сервера процессов должна быть произведена на первом сервере приложений, второй сервер приложений должен быть подключен к первому посредством настроек сервера процессов.

Взаимодействие между серверами обеспечивается с помощью защищенной сети Правительства Самарской области. При необходимости допускается установка на каждый сервер программных компонентов ViPNet Client для повышения общего уровня информационной безопасности при информационном взаимодействии.

Программные компоненты распределяются по серверам следующим образом:

- первый сервер приложений:
    - сервер процессов IBM WebSphere Process Server;
    - сервисы предоставления электронных услуг и преобразования объектов и интерфейсов;

- реестр и репозиторий сервисов;

- второй сервер приложений:
  - сервер процессов IBM WebSphere Process Server;
  - сервисы предоставления электронных услуг и преобразования объектов и интерфейсов;

- сервер БД:
  - СУБД Oracle Database Enterprise Edition10g.

7. Состав и содержание работ по созданию Прототипа

Процесс создания Прототипа представляет собой совокупность работ, необходимых и достаточных для создания информационной системы, соответствующей предъявленным требованиям. Состав и содержание работ по созданию Прототипа представлено в таблице 4.

Таблица 4 – Состав работ по созданию Прототипа

	Работа	**Результат работ**	**Ответственный**
1	Обследование проектной документации систем, вовлеченных в функционирование ИШ ЭП СО, проектирование Прототипа ИШ ЭП СО	1. Спецификация требований к прототипу информационной системы ИШ ЭП СО в соответствии с требованиями к результатам работ, указанными в Техническом задании	Исполнитель
2	Разработка программного обеспечения Прототипа	1. Инсталляционный комплект программного обеспечения, подготовленный для тестирования	Исполнитель
3	Внутреннее тестирование и корректировка программного обеспечения ИШ ЭП СО и документации на	1. Инсталляционный комплект программного обеспечения, подготовленный для установки 2. Руководство по	Исполнитель

	ИШ ЭП СО	инсталляции	
4	Монтажные работы: подготовка необходимого технического обеспечения: серверов, сетевого оборудования, выделенной электрической сети (в соответствии с требованиями, указанными в разделах 3 и 5 настоящего документа)	1. Подготовленная техническая инфраструктура	Заказчик
5	Подготовка необходимого программного обеспечения и интеграционной платформы (в соответствии с требованиями, указанными в разделах 4 и 5 настоящего документа)	1. Подготовленное программное обеспечение	Заказчик

6	Разработка плана демонстрации Прототипа информационной системы ИШ ЭП СО	1. План демонстрации Прототипа информационной системы ИШ ЭП СО	Исполнитель
7	Инсталляция и конфигурирование программного обеспечения ИШ ЭП СО. Публикация сервисов услуг, реализуемых в 2009 году, на Прототипе	1. Установленное программное обеспечение Прототипа 2. Опубликованные сервисы РН СО, ФНС России, Управления ГИБДД	Исполнитель
8	Демонстрация Прототипа	1. Протокол по результатам демонстрации Прототипа	Исполнитель Заказчик
9	Корректировка прототипа ИШ ЭП СО по итогам демонстрации и подготовка рекомендаций по развитию программно-аппаратной инфраструктуры ИШ ЭП СО	1. Измененная версия программного обеспечения информационной системы ИШ ЭП СО 2. Рекомендации по развитию программно-аппаратной инфраструктуры ИШ ЭП СО	Исполнитель

8. Список используемых сокращений

Сокращение	Расшифровка
GUID	Globally Unique Identifier
OCSP	Online Certificate Status Protocol
UDDI	Universal Description, Discovery and Integration
WSDL	Web Services Definition Language
XML	Extensible Markup Language
XSD	XML Schema Definition
БД	База данных
ВЭС	Выделенная электрическая сеть
ИС	Информационная система
ИШ ЭП СО	Интеграционная шина электронного правительства Самарской области
ЛВС	Локальная вычислительная сеть
НСИ	Нормативно-справочная информация
СУБД	Система управления базами данных
РУЦ	Региональный удостоверяющий центр Правительства Самарской области
ФЛК	Форматно-логический контроль
ЩР СГЭ	Щит распределительный системы гарантированного электропитания
ЭП СО	Электронное правительство Самарской области
ЭУ	Электронная услуга
ЭЦП	Электронная цифровая подпись

9. Связанные документы

1. Спецификация требований к интерфейсам взаимодействия между компонентами архитектуры ЭП СО в рамках оказания электронных услуг
2. Web Services Security: SOAP Message Security 1.1 (WS-Security 2004)
3. Спецификация требований к механизмам постановки и проверки ЭЦП
4. Общесистемные справочники и классификаторы, хранимые в информационной системе ИШ ЭП СО

ЛИСТ ИЗМЕНЕНИЙ

№ п/п	Дата	Автор	Содержание изменения