Содержание

[1 Вводная часть 3](#_Toc154417105)

[1.1 Цель 3](#_Toc154417106)

[1.2 Назначения 3](#_Toc154417107)

[1.3 Определения, сокращения, аббревиатуры 4](#_Toc154417108)

[1.4 Ссылки 6](#_Toc154417109)

[1.5 Обзор 7](#_Toc154417110)

[2 Общая часть 9](#_Toc154417111)

[2.1 Перспективы использования продукта 9](#_Toc154417112)

[2.2 Функции продукта 9](#_Toc154417113)

[2.3 Общие ограничения 12](#_Toc154417114)

[2.4 Предположения и зависимости 13](#_Toc154417115)

[3 Конкретные требования 14](#_Toc154417116)

[3.1 Описание сервиса 14](#_Toc154417117)

[3.1.1 Входная информация 14](#_Toc154417118)

[3.1.2 Обработка 14](#_Toc154417119)

[3.1.3 Выходная информация 16](#_Toc154417120)

[3.2 Безопасность 16](#_Toc154417121)

[3.2.1 Требования к защите информации от несанкционированного доступа 17](#_Toc154417122)

[3.2.2 Требования к мониторингу и журналированию событий 18](#_Toc154417123)

[3.2.3 Требования к формату Журнала логирования 19](#_Toc154417124)

[3.2.4 Описание процесса проверки и формирования ЭЦ 20](#_Toc154417125)

[3.2.5 Требования к алгоритму формирования ЭЦ 20](#_Toc154417126)

[3.2.6 Требования к структуре файла, подписанного ЭЦП 21](#_Toc154417127)

[3.2.7 Блокировка соединения со стороны ВШЭП/ШЭП 21](#_Toc154417128)

[3.3 Другие требования 22](#_Toc154417129)

[3.3.1 Функционирование 22](#_Toc154417130)

[3.3.2 Требования по адаптации к местоположению 23](#_Toc154417131)

[ПРИЛОЖЕНИЕ 1 24](#_Toc154417132)

[ПРИЛОЖЕНИЕ 2 38](#_Toc154417133)

[ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ 45](#_Toc154417134)

[ЛИСТ СОГЛАСОВАНИЯ 46](#_Toc154417135)

# Вводная часть

## Цель

Целью создания настоящего документа является:

* Документирование требований к взаимодействию, предъявляемых в части оптимизации и автоматизации бизнес-процессов по получению и отправке ЭД.
* Выработка у всех заинтересованных в разработке взаимодействия лиц единого понимания поведения взаимодействия при различных условиях;
* Разработка основополагающего документа для определения степени соответствия Взаимодействия установленным требованиям;
* Создание основы для написания программного кода.

Целью создания настоящего взаимодействия является получения сторонними информационными системами окончательных версий проектно-сметной документации по запросу через SmartBridge с учетом прав доступа к документации.

Документ разработан в соответствии со СТ РК 1090-2002. По мере выполнения работ по проекту, стороны могут уточнять требования к программному обеспечению.

## Назначения

Назначением настоящего документа является описание требований, предъявляемых в процессе интеграции ЕИСКВЭ и «ХХХХХХХХХХ».

Настоящий документ предназначен для широкого круга лиц, к которым относятся специалисты, входящие в группу реализации проекта со стороны владельцев интегрируемых систем:

- специалисты, входящие в группу реализации проекта со стороны Заказчика;

- лица, ответственные за подготовку графиков работ, расчетов затрат и ресурсов;

- разработчики программного обеспечения;

- специалисты тестирования;

- специалисты по сопровождению и поддержке Системы.

## Определения, сокращения, аббревиатуры

Основные понятия и сокращения, которые используются в настоящем документе, приведены в Таблице 1.

Таблица 1. Основные понятия, сокращения, аббревиатуры

|  |  |
| --- | --- |
| **Термин** | **Описание** |
| **SOAP** | Простой протокол доступа к объектам (SimpleObjectAccessProtocol) – протокол, основанный на XML для передачи сообщений при интеграции ИС |
| **Web–сервис** | Приложение или блок находящегося на web-сервере выполняемого кода, функционирование которого основано на применении стандартных форматов XML |
| **WSDL** | Web Service Definition Language – стандарт описания интерфейсов веб-сервисов |
| **XML** | eXtensibleMarkupLanguage, Расширяемый язык разметки, предназначенный для обмена информацией между программами и для хранения структурированных данных |
| **ЕИСКВЭ, РК** | Единая информационная система комплексной вневедомственной экспертизы |
| **СЭППСД, ЛК** | Система электронного приема проектно-сметной документации |
| **HTTP, HTTPS** | Hypertext Transfer [Transport] Protocol (Secure), Протокол передачи гипертекста; |
| **БИН** | Бизнес-идентификационный номер |
| **Владелец сервиса** | Собственник или владелец объекта информатизации, предоставляющий интеграционный сервис. Информационная система Владельца сервиса является источником данных, а также стороной, которая принимает сообщения от системы-инициатора информационного взаимодействия |
| **ВШЭП** | Внешний шлюз «электронного правительства» -это подсистема ШЭП, предназначенная для обеспечения взаимодействия информационных систем, находящихся в единой транспортной среде государственных органов, с информационными системами, находящимися вне единой транспортной среды государственных органов (т.е. в сети Интернет) |
| **ЕТС ГО** | Единая транспортная среда государственных органов - это сеть телекоммуникаций, входящая в информационно-коммуникационную инфраструктуру "электронного правительства" и предназначенная для обеспечения взаимодействия локальных (за исключением локальных сетей, имеющих доступ к Интернету), ведомственных и корпоративных сетей телекоммуникаций государственных органов, их подведомственных организаций и органов местного самоуправления, а также иных субъектов информатизации, определенных уполномоченным органом, с соблюдением требуемого уровня информационной безопасности |
| **Журнал логирования** | Файлы, содержащие информацию о работе системы, используемую для мониторинга ее работы и выявления причин, в случае возникновения сбоя |
| **ИИН** | Индивидуальный идентификационный номер |
| **Интеграционный сервис** | Способ информационного взаимодействия объектов информатизации |
| **ИС** | Информационная (- ые) система (-ы) - организационно-упорядоченная совокупность информационно-коммуникационных технологий, обслуживающего персонала и технической документации, реализующих определенные технологические действия посредством информационного взаимодействия и предназначенных для решения конкретных функциональных задач |
| **ИС ИИС** | Информационная система инициатора интеграционного сервиса – владельца объекта информатизации, инициирующего запрос на предоставление интеграционного сервиса |
| **Клиент сервиса** | Собственник или владелец объекта информатизации, использующего интеграционный сервис Владельца сервиса. Информационная система Клиента сервиса является получателем данных, а также инициатором информационного взаимодействия |
| **Ключ сервиса** | Уникальный идентификатор, под которым веб-сервис опубликован на ШЭП/ВШЭП |
| **Объект автоматизации** | Электронные информационные ресурсы, программное обеспечение, интернет-ресурс и информационно-коммуникационная инфраструктура |
| **ПСД** | Проектно-сметная документация |
| **Система** | Комплексный инструмент автоматизации приема, обработки и выдачи документации при экспертизе проектов строительства – СЭППСД и ЕИСКВЭ  |
| **ШЭП** | Шлюз «электронного правительства» - это информационная система, предназначенная для интеграции объектов информатизации «электронного правительства» с иными объектами информатизации «электронного правительства». |
| **ЭЦП** | Электронно-цифровая подпись |

## Ссылки

Настоящий документ основывается на следующих основных нормативно-правовых актах:

1. Закон Республики Казахстан «Об электронном документе и электронной цифровой подписи» от 7 января 2003 года № 370;
2. Закон Республики Казахстан «Об информатизации» от 24 ноября 2015 года № 418-V;
3. Государственный стандарт Республики Казахстан СТ РК 1073-2007 «Средства криптографической защиты. Общие технические требования»;
4. Национальный стандарт Республики Казахстан СТ РК ИСО/МЭК 27002-2015 «Информационная технология. Методы и средства обеспечения безопасности. Свод правил по средствам управления защитой информации» (далее – СТ РК ИСО/МЭК 27002-2015);
5. СТ РК ИСО/МЭК 27001-2015 Информационные технологии. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования.
6. Национальный стандарт Республики Казахстан СТ РК ГОСТ Р 50739-2006 Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования;
7. Постановление Правительства Республики Казахстан «Об утверждении Правил документирования, управления документацией и использования систем электронного документооборота в государственных и негосударственных организациях» от 31 октября 2018 года № 703;
8. Постановление Правительства Республики Казахстан «Об утверждении единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности» от 20 декабря 2016 года № 832;
9. Приказ и.о. Министра информации и коммуникаций Республики Казахстан «Об утверждении Правил интеграции объектов информатизации «электронного правительства» от 29 марта 2018 года № 123 (далее – Правила интеграции);
10. Приказ Министра по инвестициям и развитию Республики Казахстан «Об утверждении Правил проверки подлинности электронной цифровой подписи» от 9 декабря 2015 года № 1187;
11. Схема взаимодействия объектов информатизации посредством внешнего шлюза «электронного правительства», утвержденная МИК РК от 23 мая 2018 года.

## Обзор

Настоящий документ включает следующие разделы:

* Раздел 1 «Вводная часть»;
* Раздел 2 «Общая часть»;
* Раздел 3 «Конкретные требования»;
* Приложения.

Раздел 1 «Вводная часть» представляет собой обзор, описывающий цель и общее назначение настоящего документа, включает определения, обозначения и аббревиатуры, а также ссылки на используемые документы.

Раздел 2 «Общая часть» включает в себя общие сведения по разрабатываему взаимодействию, перспективы использования продукта, функции, известные ограничения, предположения и зависимости.

В разделе 3 «Конкретные требования» приводятся конкретные требования к интегрируемым Системам.

Приложения содержат дополнительные сведения, а также информацию разъяснительного характера, упрощающую понимание настоящего документа.

# Общая часть

Порядок интеграции ШЭП/ВШЭП с информационными системами должен соответствовать Правилам интеграции объектов информатизации «электронного правительства», утвержденным приказом и.о. Министра информации и коммуникаций Республики Казахстан от 29 марта 2018 года № 123.

Интеграция должна соответствовать положениям пп.7) и пп.11) п.139 Единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности, утвержденные Постановлением Правительства Республики Казахстан от 20 декабря 2016 года № 832.

## Перспективы использования продукта

SOAP сервис передачи файлов по градостроительным и строительным проектам предназначен для получения сторонними информационными системами окончательных версий проектно-сметной документации по запросу через SmartBridge с учетом прав доступа к документации.

## Функции продукта

Реализация интеграции предоставит возможность для получения сторонними информационными системами окончательных версий проектно-сметной документации по запросу через SmartBridge с учетом прав доступа к документации.

Схема взаимодействия показана на рис.1.

**Основной сценарий взаимодействия:**

1) ИС ИИС инициирует в ВШЭП запрос, заверенный транспортной ЭЦП ИС ГО, с атрибутами, указанными в Приложение 1.

2) Запрос ИС ИИС поступает в ВШЭП. ВШЭП проводит валидацию на предмет подлинности транспортной ЭЦП.

3) ВШЭП проводит валидацию запроса (проверку конверта на соответствие формату сообщения для асинхронного канала). Описание форматов взаимодействия с ВШЭП/ШЭП указаны в Приложение 1 к данному документу.

4) ВШЭП проводит авторизацию Инициатора взаимодействия, проверяет права на указанное взаимодействие (иначе Альтернативный сценарий 1).

5) Проверки прошли успешно. ВШЭП фиксирует сведения о запросе в журнал трассировки сообщения.

6) ВШЭП отправляет запрос в ШЭП.

7) ШЭП проводит валидацию запроса.

8) Валидация на стороне ШЭП прошла успешно. ШЭП снимает ЭЦП, подписывает сообщение ЭЦП владельца ШЭП с применением спецификации WS Security. ШЭП отправляет запрос в ЕИСКВЭ (иначе Альтернативный сценарий 2).

9) ЕИСКВЭ принимает запрос, проводит валидацию полученного запроса на предмет целостности атрибутов согласно требованиям, описанным в Приложение 1.

10) Проверка на стороне ЕИСКВЭ прошла успешно. ЕИСКВЭ обрабатывает полученные сведения. (иначе Альтернативный сценарий 3).

11) ЕИСКВЭ формирует ответное сообщение, заверяет ответ системной ЭЦП.

12) ЕИСКВЭ направляет ответ в ВШЭП/ШЭП.

13) ШЭП проводит валидацию ответного сообщения, проверку ЭЦП информационной системы.

14) Валидация на стороне ШЭП прошла успешно. ШЭП снимает ЭЦП, подписывает сообщение ЭЦП владельца ШЭП с применением спецификации WS Security. (иначе Альтернативный сценарий 4).

15) ШЭП фиксирует сведения об ответном сообщении в журнал трассировки сообщения. ШЭП передает ответное сообщение в ВШЭП.

16) ВШЭП проверяет ЭЦП информационной системы.

17) Проверка на стороне ВШЭП прошла успешно. ВШЭП передает ответное сообщение в ИС ИИС (иначе Альтернативный сценарий 5).

**Альтернативные сценарии к процессу:**

**Альтернативный сценарий 1.** Валидация на стороне ВШЭП прошла неуспешно:

1) ВШЭП возвращает запрос в ИС ИИС с информацией об ошибке.

**Альтернативный сценарий 2.** Валидация на стороне ШЭП прошла неуспешно:

1) ШЭП возвращает запрос во ВШЭП с информацией об ошибке.

2) ВШЭП транслирует сообщение об ошибке в ИС ИИС.

**Альтернативный сценарий 3.** Валидация на стороне ЕИСКВЭ прошла неуспешно:

1) ЕИСКВЭ возвращает запрос в ИШ с информацией об ошибке.

2) ШЭП транслирует сообщение об ошибке во ВШЭП.

3) ВШЭП транслирует сообщение в ИС ИИС с информацией об ошибке.

4) ИС ИИС принимает и обрабатывает сообщение об ошибке.

**Альтернативный сценарий 4**. Валидация ответа ЕИСКВЭ на стороне ШЭП прошла неуспешно:

1) ШЭП возвращает запрос в ЕИСКВЭ с информацией об ошибке.

2) ЕИСКВЭ принимает и обрабатывает сообщение об ошибке.

**Альтернативный сценарий 5.** Валидация ответа ЕИСКВЭ на стороне ВШЭП прошла неуспешно:

1) ВШЭП возвращает запрос в ШЭП с информацией об ошибке.

2) ШЭП транслирует сообщение в ЕИСКВЭ с информацией об ошибке.

3) ЕИСКВЭ принимает и обрабатывает сообщение об ошибке.



Рис. 1 Схема взаимодействия

## Общие ограничения

Размер передаваемого пакета между объектами информатизации посредством ВШЭП/ШЭП не должен превышать 15 МБ.

Таблица 2 Набор требований по производительности и надежности

|  |  |  |
| --- | --- | --- |
| **№** | **Контролируемый показатель** | **Ограничение** |
| 1 | Максимальное время обработки запроса при асинхронном взаимодействии | Время предоставления результата по запросу на асинхронном сервисе, зависит от реализации каждого интеграционного сервиса |
| 2 | Пиковая нагрузка | 2000 запросов в час |
| 3 | Номинальная нагрузка | 360 запросов в час |
| 4 | Среднее время работы без сбоев | 365/7/24 |
| 5 | Время на восстановление работоспособности | 3 часа |

## Предположения и зависимости

Внесение изменений в действующее законодательство РК может потребовать доработки функциональных возможностей, структур БД или логики обработки данных объектов интеграции. В документ могут быть внесены изменения в состав данных согласно утвержденным правилам интеграции.

# Конкретные требования

Функциональные требования обеспечиваются реализацией сценариев взаимодействия с сервисом

Информационное взаимодействие между ЕИСКВЭ и «ХХХХХХХХХХ» осуществляется посредством ВШЭП, ШЭП, ЕИСКВЭ в соответствии с настоящими техническими требованиями (схема взаимодействия приведена в разделе 2.2 «Функции продукта»).

## Описание сервиса

### Входная информация

Таблица 3

|  |  |  |  |
| --- | --- | --- | --- |
| **Наименование поля** | **Формат** | **Ограничение** | **Обязательность** |
| ApiKey | Символьный |  | Да |
| Номер заключения | Символьный |  | Да |
| Дата заключения | Дата | ДД.ММ.ГГГГ | Да |
| Наименование файла согласия | Текстовый |  | Нет |
| Файл согласия | Ссылка |  | Нет |
| Номер части ПСД | Числовое, целое |  | Да |

### Обработка

Информационный обмен между ЕИСКВЭ и интегрируемыми системами осуществляется в режиме запрос-ответ.

Входная информация, указанная в Таблице 3 должна содержаться в requestData запроса (согласно таблице 5 Приложения 1).

Выходная информация, указанная в Таблице 4 должна содержаться в responseData ответа (согласно таблице 6 Приложения 1).

Инициатором отправки сведений из ЕИСКВЭ является интегрируемая система.

Информационный обмен между ЕИСКВЭ и интегрируемой системой осуществляется посредством ВШЭП и ШЭП и производится через информационные сервисы с использованием технологии веб-сервисов посредством обмена данными путем передачи SOAP-сообщений. В качестве транспорта доставки SOAP-сообщений выступает защищенный посредством сертификатов SSL, выданных НУЦ РК, протокол HTTPS.

Информационный обмен должен осуществляться в асинхронном режиме.

При информационном взаимодействии, сообщения должны подразделяться на следующие два типа: запрос и ответ. Инициализирующим информационный обмен сообщением является сообщение типа «запрос». На сообщение типа «запрос» получатель должен выслать отправителю сообщение типа «ответ».

Сообщения и бизнес-данные, формируемые при обмене, должны быть подписаны цифровым сертификатом, регистрационное свидетельство которого выпущено НУЦ РК.

Сообщение подписывается ЭЦП владельца ИС отправителя с применением спецификации WS Security (транспортная подпись).

Структура подписанного ЭЦП XML-файла должна соответствовать спецификации консорциума W3C «XML - Signature Syntax and Processing» (Синтаксис и обработка подписи XML).

Для передачи данных используется транспортный протокол TCP/IP.

Язык описания WSDL.

Язык XSD для описания структур данных, подписываемых ЭЦП.

Факты отправки/получения/сбоя доставки сообщений фиксируются в протоколе информационного обмена на серверах ЕИСКВЭ, интегрируемой системы, ВШЭП и ШЭП. Сервисы информационного взаимодействия между ЕИСКВЭ и интегрируемой системы записывает в Log-журналах систем факт получения/отправки сообщений с соответствующим кодом. При заполнении Log-журнала системы, данные архивируются по мере заполнения. В рамках ЕИСКВЭ факты должны фиксироваться в отдельном журнале событий.

ИС получателя сообщения проверяет целостность сообщения, ЭЦП на действительность, истекший срок действия ЭЦП, отозванность и соответствие БИН, указанного в ЭЦП, с БИН ЭЦП владельца ШЭП.В случае, если проверка не пройдена в качестве ответа на запрос необходимо направлять сообщение об ошибке согласно таблицам 7, 8.

После проверки ЭЦП ЕИСКВЭ выполняет проверку бизнес-данных с учетом настройки сведений о сервисе для интегрируемой системы «ХХХХХХХХХХ», в том числе касательно обязательности предоставления согласия заказчика КВЭ.

ЕИСКВЭ должен предоставлять информацию согласно таблице 4.

Архив «Окончательной версии ПСД» передается только в случае «Корректность = 1» после выполнения вышеуказанных проверок.

Допускается отправка многотомных архивов (одно сообщение содержит один том архива). Один том архива не должен быть больше 15 мегабайт.

При наличии нескольких томов для архива ПСД, каждый том запрашивается отдельным запросом, указав в запросе номер тома.

Фиксация всех временных параметров в процессе обработки сообщений производится по времени г. Астана.

### Выходная информация

Таблица 4

|  |  |  |  |
| --- | --- | --- | --- |
| **Наименование**  | **Формат** | **Ограничение** | **Обязательность** |
| Код Корректности | Символьный | Справочник. 0 – заключения не существует1 – заключение существует2 – заключение аннулировано3 – доступ запрещён4 – файл согласия по ссылке не найден5 – нет АВР по проекту 6 - не подписан авторский договор7 – архив окончательной версии ПСД отсутствует8– доступ к ПСД отключен | Да |
| Номер заключения | Символьный |  | Да |
| Дата заключения | Дата |  | Да |
| БИН/ИИН заявителя | Символьный, 12 цифр | Указывается при наличии сведений о заключении | Нет |
| Окончательная версия ПСД  | Файл | При необходимости разбивка на пакеты объемом не более 15Мб в формате Base64 | Нет |
| Имя тома  | Символьный |  | Да |
| Размер тома | Числовое |  | Да |
| Данные тома | Массив |  | Да |
| Хэш | MD5 |  | Да |
| Количество томов | Числовое, целое |  | Да |

## Безопасность

Для реализации работоспособности сервиса следующий набор требований по информационному обеспечению:

* Должно быть обеспечено журналирование действий пользователей, влияющих на информационную безопасность, и журналирование критичных событий программного обеспечения;

### Требования к защите информации от несанкционированного доступа

Защита от несанкционированного доступа должна обеспечивать:

* идентификацию пользователя, основанную на цифровых сертификатах инфраструктуры открытых ключей;
* авторизацию пользователя для доступа к информационно-вычислительным ресурсам, требующим наличия соответствующих разрешений;
* системы должны иметь SSL сертификаты;
* структура подписанного ЭЦП XML-файла, должна соответствовать спецификации консорциума W3C «XML - SignatureSyntaxandProcessing» («Синтаксис и обработка подписи XML»), см. ссылку <http://www.w3.org/TR/xmldsig-core/>.

С целью контроля событий нарушений ИБ обеспечить регистрацию события:

1. должна проводится мониторинг событий, связанных с нарушением ИБ, и анализ результатов мониторинга;

2. должна регистрироваться события, связанные с состоянием ИБ, и выявляются нарушения путем анализа журналов событий, в том числе:

− журналов событий операционных систем;

− журналов событий систем управления базами данных;

− журналов событий антивирусной защиты;

− журналов событий прикладного ПО;

− журналов событий телекоммуникационного оборудования;

− журналов событий систем обнаружения и предотвращения атак;

− журналов событий системы управления контентом.

3. журналы необходимо хранить в течение срока, указанного в нормативно-технической документации в сфере обеспечения информационной безопасности, но не менее трех лет, а также быть в оперативном доступе не менее трех месяцев;

4. при журналировании событий необходимо обеспечивать синхронизацию времени с инфраструктурой источника времени;

5. должна обеспечиваться защита журналов регистрации событий от вмешательства и неавторизированного доступа;

должна обеспечиваться внедрение формализованной процедуры информирования об инцидентах ИБ и реагирования на инциденты ИБ.

### Требования к мониторингу и журналированию событий

Журнал событий должен вестись в соответствии с требованиями стандарта СТ РК ИСО/МЭК 27002-2015 и со схемой взаимодействия объектов информатизации посредством шлюза «электронного правительства», утвержденной приказом Вице-министра информации и коммуникаций Республики Казахстан от 23 апреля 2018 года.

Следующие события должны подлежать обязательному журналированию:

* Авторизация (вход и выход) пользователей, успешные и неуспешные попытки авторизации;
* Создание, копирование, перемещение, удаление, модификация локальных учетных записей и конфигурационных файлов;
* Неудавшиеся или отвергнутые действия пользователя;
* Получение пользователем доступа к объектам доступа.
* Требования к формату файла:
* Журнал логирования должен быть текстовом в формате (нельзя использовать журнал логирования в бинарном формате);
* Журнал логирования должен иметь расширения следующих видов: \*.txt,\*.log;
* Расположение файлов журналов событий должны быть в отдельной папке в корневой директории ПО;
* Наименование папки с файлами журналов логирования должно описывать информацию о хранения журналов логирования.
* Журнал логирования в обязательном порядке должен содержать следующие поля:
* Дата и время (формат даты: ДД:ММ:ГГГГ, формат времени: ЧЧ:ММ:СС);
* Наименование источника события (сервис/служба);
* Имя учетной записи/ID пользователя;
* IP-адрес клиента;
* Время начала операции;
* Время окончания операции;
* Уровень события (определяется Оператором);
* Категория события (определяется Оператором);
* Описание события.

При журналировании событий необходимо обеспечивать:

− защиту журналов регистрации событий от вмешательства и неавторизированного доступа;

− внедрение формализованной процедуры информирования об инцидентах ИБ и реагирования на инциденты ИБ.

Журналы необходимо хранить в течение срока, указанного в нормативно-технической документации в сфере обеспечения информационной безопасности, но не менее трех лет, а также быть в оперативном доступе не менее трех месяцев.

При журналировании событий необходимо обеспечивать синхронизацию времени с инфраструктурой источника времени.

### Требования к формату Журнала логирования

Для событий, фиксируемых в журналах необходимо определять формат записи. Значения полей необходимо разделять символами-разделителями, в случае если поле имеет длинный формат и в содержании поля присутствует символ-разделитель, применять символы-ограничители полей.

При журналировании событий необходимо обеспечивать синхронизацию времени сервера с инфраструктурой источника времени.

Журнал логирования должен быть в текстовом формате, каждое событие должно содержать всю информацию в одной строке. Допускается хранение журналов в формате XML, а также в табличной форме в БД.

Для журналов должна использоваться кодировка UTF-8.

В один файл журнала не допускается запись событий, имеющих разные форматы данных.

В Журнале логирования необходимо использовать пары ключ-значение. Если значение содержит пробелы, их необходимо поместить в кавычки.

В Журнале логирования необходимо использовать уникальные идентификаторы (ID).

Не изменять уникальные идентификаторы (Идентификаторы транзакций, идентификаторы пользователя), и их формат, на всем пути следования транзакции.

Уровень логирования должен быть расширенным. Необходимо добавлять информацию о входах и выходах пользователя, действия пользователя, транзакции, информацию о времени и так далее.

В Журналах логирования необходимо использовать категории события, следующие имеющие значения:

* INFO;
* WARN;
* ERROR;
* DEBUG.

При возникновении исключительной ситуации сервис должен сохранить информацию о ней в журнале событий и сформировать ответ с информацией об ошибочной ситуации.

### Описание процесса проверки и формирования ЭЦ

Система должна предусматривать использование ЭЦП при подписании запросов внутри Системы. При использовании ЭЦП система должна учесть:

* Проверкe подлинности ЭЦП;
* Проверкe срока использования;
* Статус отозванности (ключ не должен быть отозванным).

Регистрационное свидетельство должно быть выдано на имя МЦРИОАП РК. Должна производиться проверка ИИН/БИН Отправителя с ИИН/БИН в регистрационном свидетельстве.

− Должно быть Использование ЭЦП интегрируемыми объектами интеграции при подписании запроса/ответа в рамках взаимодействия;

− Использование ЭЦП пользователя объекта интеграции при его участии в формировании запроса/ответа в рамках взаимодействия интегрируемых ОИ;

− Подтверждением авторства сообщений должен быть положительный результат проверки соответствия транспортной подписи регистрационным свидетельством ЭЦП владельца объекта интеграции, направившего сообщение.

− Проверка транспортной подписи осуществляется с соблюдением следующих процедур:

• проверка принадлежности ЭЦП НУЦ РК отправителю сообщения;

• проверка действительности ЭЦП выданная НУЦ РК.

### Требования к алгоритму формирования ЭЦП

Проверка ЭЦП должна осуществляться в соответствии с требованиями Приказа Министра по инвестициям и развитию Республики Казахстан от 9 декабря 2015 года № 1187 «Об утверждении Правил проверки подлинности электронной цифровой подписи».

Алгоритм формирования ЭЦП должен соответствовать ГОСТ 34.310-2004 или ГОСТ Р 34.10-2015.

### Требования к структуре файла, подписанного ЭЦП

Структура подписанного ЭЦП XML-файла должна соответствовать спецификации консорциума World Wide Web Consortium (Консорциум Всемирной паутины, организация, разрабатывающая и внедряющая технологические стандарты для Всемирной паутины) "XML-Signature Syntax and Processing" (синтаксис и обработка подписи XML).

      ЭЦП систем с применением Web Service Security (безопасность веб-сервисов, стандарт применения функций безопасности при обмене сообщениями между веб-сервисами SOAP), выданных НУЦ РК.

Обмен данными между системами должен соответствовать следующим форматам:

1) Использовать HTTPS, с применением регистрационных свидетельств SSL, выданных НУЦ РК, в качестве транспортного протокола;

2) Использовать SOAP протокол (Simple Object Access Protocol) в качестве протокола взаимодействия;

3) В рамках взаимодействия по протоколу SOAP, использовать ЭЦП информационной системы, выданной НУЦ РК, в соответствии спецификации WS-security;

Структура подписанного ЭЦП XML-файла должна соответствовать спецификации консорциума W3C «XML - Signature Syntax and Processing» (Синтаксис и обработка подписи XML).

### Блокировка соединения со стороны ВШЭП/ШЭП

Блокировка соединения со стороны ВШЭП/ШЭП осуществляется при следующих условиях:

* Отсутствие соединения с ОИ в течении 60 сек;
* Превышение частоты запросов в соответствии с таблицей 2 настоящего Документа;
* Наличие в запросах нарушений ИБ в соответствии с едиными требованиями в области информационно-коммуникационных технологий и обеспечения информационной безопасности.

##  Другие требования

###  Функционирование

Необходимо обеспечение бесперебойной работоспособности сервиса передачи файлов по градостроительным и строительным проектам по запросу через SmartBridge с учетом прав доступа к документации (кроме плановых и профилактических работ, системно - технических сбоев, сбоев на стороне ИС ГО и перебоев в каналах связи).

Непрерывность функционирования ЕИСКВЭ и своевременность восстановления ее работоспособности достигается:

- проведением специальных организационных мероприятий и разработкой организационно-распорядительных документов по вопросам обеспечения непрерывной работы и восстановления;

- обучением сотрудников действиям при возникновении чрезвычайных ситуаций, включая кризисное управление;

- применением различных способов резервирования аппаратных ресурсов, копирования программных и информационных ресурсов ЕИСКВЭ;

- на постоянной основе поддержанием необходимого уровня защищенности компонентов ЕИСКВЭ, непрерывным управлением и административной поддержкой корректного применения средств защиты.

***Примечание:*** *в соответствие с пунктом 90-1 ЕТ при реализации функций интеграционного взаимодействия объектов информатизации или компонентов объектов информации посредством шлюза, интеграционной шины, интеграционного компонента или интеграционного модуля обеспечиваются:*

*1) регистрация и проверка источников (точек подключений) запросов на легитимность;*

*2) проверка легитимности запросов по:*

*паролю или ЭЦП;*

 *точке подключения;*

*наличию блокировки соединения;*

*разрешенным видам запросов, определенным в регламенте интеграционного взаимодействия;*

*разрешенной частоте запросов, определенной в регламенте интеграционного взаимодействия;*

*наличию в запросах признаков нарушений информационной безопасности;*

*наличию вредоносного кода по сигнатурам;*

*3) блокировка соединения при обнаружении нарушений в протоколах обмена сообщениями при:*

*отсутствии соединения в течение времени, определенного в регламенте интеграционного взаимодействия;*

*превышении разрешенной частоты запросов на время, определенное в регламенте интеграционного взаимодействия;*

*наличии в запросах признаков нарушений информационной безопасности;*

*превышении количества ошибок аутентификации, определенного в регламенте интеграционного взаимодействия;*

*выявлении аномальной активности пользователей;*

*выявлении попыток выгрузки массивов данных;*

*4) регулярная смена паролей соединения по времени действия, определенного в регламенте интеграционного взаимодействия;*

*5) замена логина соединения при выявлении инцидентов ИБ;*

*6) сокрытие адресации ЛС внутреннего контура;*

*7) журналирование событий, включающее:*

*регистрацию событий передачи/приема информационных сообщений;*

*регистрацию событий передачи/ получения файлов;*

*регистрацию событий передачи/получения служебных сообщений;*

*применение системы управления инцидентами и событиями ИБ для мониторинга журналов событий;*

*автоматизацию процедур анализа журналов событий на наличие событий ИБ;*

*хранение журналов событий на специализированном сервере логов, доступном для администраторов только для просмотра;*

*раздельное ведение журналов событий (при необходимости) по:*

*а) текущим суткам;*

*б) соединению (каналу связи);*

*в) государственному органу (юридическому лицу);*

*г) интегрируемым объектам информатизации;*

*8) предоставление сервиса синхронизации времени для интегрируемых объектов информатизации;*

*9) программно-аппаратная криптографическая защита соединений, осуществляемых через сети передачи данных;*

*10) хранение и передача паролей соединений в зашифрованном виде;*

*11) автоматизация оповещения об инцидентах ИБ ответственных лиц интегрируемых объектов информатизации.*

###  Требования по адаптации к местоположению

Особых условий установки и эксплуатации, зависящих о местоположения программного обеспечения не предусмотрено.

# ПРИЛОЖЕНИЕ 1

**Форматы данных веб-сервиса SOAP**

**Описание сообщений асинхронного канала**

1. Интерфейс сервиса на ШЭП, ВШЭП:

**Метод для отправки сообщений на асинхронный канал ШЭП, ВШЭП** (**SendMessage):**

Запрос на предоставление сервиса (**SendMessageRequest**) содержит следующие поля:

**Таблица 5** Формат данных SendMessageRequest

| **Поле** | **Тип** | **Обязанность** | **Описание** |
| --- | --- | --- | --- |
| request | AsyncSendMessagerequest | Да | Запрос |
| messageInfo | AsyncMessageInfo | Дa | Метаданные сообщения |
| messageId | xsd: string | Да | Идентификатор сообщения в системе получателя (заполняет система получателя запроса (система отрабатывающая сообщение) |
| correlationId | xsd: string | Нет | Идентификатор цепочки сообщения в системе получателя запроса (если сообщения существует в рамках цепочки сообщений системы (отправителя) система отрабатывающая сообщение) |
| serviceId | xsd: string | Да | Идентификатор сервиса |
| messageType | xsd: string | Да | Тип сообщения:REQUEST - первое сообщения взаимодействия |
| routeId | xsd: string | Нет | Идентификатор маршрута сообщения (если есть необходимость в дополнительной маршрутизации, идентификатор по реестру, заполняется системой отправителя) |
| messageDate | xsd: dateTime | Да | Дата создания сообщения |
| sessionId | guid | Да | Идентификатор сессии ШЭП. Заполняется на ШЭП, отправителю заполнять не надо. |
| sender | SenderInfo | Да | Объект информация об отправителе (заполняется отправителем) |
| senderId | xsd: string | Да | Идентификатор отправителя (системы отправителя) |
| password | xsd: string | Да | Пароль отправителя |
| properties | property | Нет | Массив свойств, можно добавить дополнительные свойства запроса (по согласованию с ШЭП и системой получателя) |
| key | xsd: int |  | Ключ свойства |
| value | xsd: int | Нет | Значение свойства |
| messageData | messagedata | Да | Объект передачи данных |
| data | xsd: Anytype | Нет | Объект данные сообщения (формат определяется системой получателя сообщения) |

Ответ ШЭП, ВШЭП на сообщение (s**endMessageResponse**) представляет собой массив элементов со следующими полями:

**Таблица 6** Формат данных SendMessageResponse

|  |  |  |  |
| --- | --- | --- | --- |
| **Поле** | **Тип** | **Обязанность** | **Описание** |
| response | AsyncSendMessagerequest | Да | Ответ |
| messageId | xsd: string | Да | Идентификатор сообщения |
| correlationId | xsd: string | Да | Идентификатор цепочки сообщения |
| responseDate | xsd: dateTime | Да | Дата ответа |
| sessionId | Guid | Нет | Идентификатор сессии ШЭП |

Ответ об ошибке (**SendMessagefault**) представляет собой массив элементов со следующими полями:

**Таблица 7** Формат данных SendMessagefault

|  |  |  |  |
| --- | --- | --- | --- |
| **Поле** | **Тип** | **Обязанность** | **Описание** |
| ErrorInfo | ErrorInfo |  | Информация об ошибке |
| errorCode | xsd: string | Да | Код ошибки |
| errorData | xsd: string | Да | Дополнительное описание ошибки |
| errorDate | xsd: dateTime | Да | Дата ошибки |
| subError | ErrorInfo | Нет | Дочерняя ошибка |
| sessionId | guid | Нет | Идентификатор сессии в которой произошла ошибка |

Метод отправки уведомления на ШЭП, ВШЭП о доставке или не доставке сообщения (**SendDeliveryNotification**):

Запрос на уведомление представляет собой массив элементов со следующими полями (**sendDeliveryNotificationRequest**):

**Таблица 8** Формат данных SendDeliveryNotificationRequest

|  |  |  |  |
| --- | --- | --- | --- |
| **Поле** | **Тип** | **Обязанность** | **Описание** |
| request | Async SendDeliveryNotificationRequest | Да | Запрос |
| notification | DeliveryNotification | Да | Уведомления о статусе доставки сообщения |
| messageId | xsd: string | Да | Идентификатор сообщения |
| serviceid | xsd: string | Да | Идентификатор сервиса |
| notificationDate | xsd: dateTime | Да | Дата создания уведомления |
| deliveryStatus | deliveryStatusInfo | Да | Статус доставки (приема сообщения) |
| receiveStatus | xsd: string | Да | Статус доставки сообщения:MESSAGE\_NOT\_ACCTEPTED – сообщения не принятоMESSAGE\_ACCEPTED – сообщения принято |
| statusDate | xsd: dateTime | Да | Дата изменения статуса |
| resendMessage | xsd: string | Да | Повторное сообщение |
| error | ErrorInfo | Нет | Информация об ошибке |
| errorCode | xsd: string | Да | Код ошибки |
| errorData | xsd: string | Нет | Дополнительное описание ошибки |
| errorDate | xsd: dateTime | Да | Дата ошибки |
| subError | ErrorInfo | Нет | Дочерняя ошибка |
| sessionId | guid | Нет | Идентификатор сессии в которой произошла ошибка |
| requestDate | xsd: dateTime | Да | Дата запроса |
| sender | SenderInfo | Нет | Отправитель |
| senderId | xsd: string | Да | Идентификатор отправителя |
| password | xsd: string | Нет | Пароль отправителя |

Ответ на уведомление (**sendDeliveryNotificationResponse**) представляет собой массив со следующими полями:

**Таблица 9** Формат данных SendDeliveryNotificationResponse

|  |  |  |  |
| --- | --- | --- | --- |
| **Поле** | **Тип** | **Обязанность** | **Описание** |
| Response | Async SendDeliveryNotificationResponse |  | Ответ |
| notificationId | xsd: string | Да | Идентификатор сообщения |
| responseDate | xsd: dateTime | Да | Дата ответа |
| sessionId | guid | Нет | Идентификатор сессии ШЭП |

Ответ об ошибке (**SendMessageFaul**t) представляет собой массив элементов со следующими полями:

**Таблица 10** Формат данных SendMessageFault

|  |  |  |  |
| --- | --- | --- | --- |
| **Поле** | **Тип** | **Обязанность** | **Описание** |
| ErrorInfo | ErrorInfo |  | Информация об ошибке |
| errorCode | xsd: string | Да | Код ошибки |
| errorData | xsd: string | Да | Дополнительное описание ошибки |
| errorDate | xsd: dateTime | Да | Дата ошибки |
| subError | ErrorInfo | Нет | Дочерняя ошибка |
| sessionId | guid | Нет | Идентификатор сессии в которой произошла ошибка |

Метод получения статуса сообщения с ШЭП, ВШЭП (**GetMessageStatus**)

Запрос на статус сообщения (**GetMessageStatusRequest**) представляет собой массив элементов со следующими полями:

**Таблица 11** Формат данных GetMessageStatusRequest

|  |  |  |  |
| --- | --- | --- | --- |
| **Поле** | **Тип** | **Обязанность** | **Описание** |
| request | AsyncGetmessagestatus | Да | Запрос |
| messageId | xsd: string | Да | Идентификатор сообщения |
| requestDate | xsd: dateTime | Да | Дата запроса |
| sender | senderinfo | Да | Объект информация об отправителе (заполняется отправителем) |
| senderId | xsd: string | Да | Идентификатор отправителя (системы отправителя) |
| password | xsd: string | Нет | Пароль отправителя |
| properties | property | Нет | Массив свойств запроса |
| key | xsd: int |  | Ключ свойства |
| value | xsd: int | Нет | Значение свойства |

В ответе на запрос на статус (**getMessageStatusResponse)** должна быть возвращена структура следующего вида:

**Таблица 12** Формат данных GetMessageStatusResponse

|  |  |  |  |
| --- | --- | --- | --- |
| **Поле** | **Тип** | **Обязанность** | **Описание** |
| response | Async GetmessagestatusResponse |  | Ответ |
| messageState | messageState | Да | Состояние сообщения |
| responseDate | xsd: dateTime | Да | Дата ответа |
| sessionId | xsd: string | Нет | Идентификатор сессии на ШЭП |
| status | MessagestatusInfo |  | Объект "Информация о статусе" |
| statusсode | xsd: int | Да | Код статуса сообщения |
| statusmessage | xsd: string | Да | Сообщение статуса |
| statusDate | xsd: dateTime | Да | Дата изменения статуса |

В случае возникновении ошибки в системе, передается сообщение об ошибке (**SendMessageFault**), которая представляет собой массив элементов со следующими полями:

**Таблица 13** Формат данных SendMessageFault

|  |  |  |  |
| --- | --- | --- | --- |
| **Поле** | **Тип** | **Обязанность** | **Описание** |
| ErrorInfo | ErrorInfo |  | Информация об ошибке |
| errorCode | xsd: string | Да | Код ошибки |
| errorData | xsd: string | Да | Дополнительное описание ошибки |
| errorDate | xsd: dateTime | Да | Дата ошибки |
| subError | ErrorInfo | Нет | Дочерняя ошибка |
| sessionId | guid | Нет | Идентификатор сессии в которой произошла ошибка |

Метод выборки сообщений с ШЭП (GetMessages) осуществляется по параметрам:

* идентификатору сообщения + получателю (только для запросившего)+идентификатору сервиса;
* идентификатору цепочки сообщений + получателю (только для запросившего) + идентификатору сервиса;
* получателю (только для запросившего) + идентификатору сервиса.

Параметр GetMessagesRequest

Запрос содержит следующие поля:

**Таблица 14** Формат данных GetMessageRequest

|  |  |  |  |
| --- | --- | --- | --- |
| **Поле** | **Тип** | **Обязанность** | **Описание** |
| request | Async GetmessagesRequest | Да | Метаданные запроса |
| messageId | xsd: string | Да | Идентификатор сообщения |
| correlationId | xsd: string | Нет | Идентификатор цепочки сообщения |
| requestdate | xsd: dateTime | Нет | Дата запроса |
| serviceId | xsd: string | Да | Идентификатор сервиса |
| sender |  Senderinfo  | Нет | Объект информация об отправителе (заполняется отправителем) |
| senderId | xsd: string |  | Идентификатор отправителя (системы отправителя) |
| password | xsd: string |  | Пароль отправителя |
| amount | xsd: int | Нет | Максимальное кол-во сообщений в выборке.Если данное поле отсутствует в запросе или равно 0, то будет принято настроенное на ШЭП значение |
| properties | Property | Да | Массив свойств, можно добавить дополнительные свойства запроса (по согласованию с ШЭП и системой получателя |
| key |  xsd: string  | Да | Ключ свойства |
| value | xsd: string | Да | Значение свойства |

Ответ getMessagesResponse со следующими полями:

**Таблица 15** Формат данных GetMessageResponse

|  |  |  |  |
| --- | --- | --- | --- |
| **Поле** | **Тип** | **Обязанность** | **Описание** |
| response | Async GetmessageResponse | Да | Ответ |
| responseDate | xsd: dateTime | Да | Дата ответа |
| sessionId | xsd: string | Да | Идентификатор сессии на ШЭП |
| messages | Asynmessage | Нет |  |
| messageInfo | Asynmessageinfo | Да | Метаданные сообщения |
| messageId | xsd: string | Нет | Идентификатор сообщения |
| correlationId | xsd: string | Да | Идентификатор цепочки |
| serviceId | xsd: string | Да | Идентификатор сервиса |
| messageType | xsd: string | Да | Тип сообщения:REQUEST - первое сообщения взаимодействия |
| routeId | xsd: string | Нет | Идентификатор маршрута сообщения (если есть необходимость в дополнительной маршрутизации, идентификатор по реестру, заполняется системой отправителя) |
| messageDate | xsd: dateTime | Да | Дата создания сообщения |
| sessionId | guid | Нет | Идентификатор сессии ШЭП. Заполняется на ШЭП, отправителю заполнять не надо. |
| Sender | SenderIndo | Да | Объект информация об отправителе (заполняется отправителем) |
| senderId | xsd: string | Да | Идентификатор отправителя (системы отправителя) |
| password | xsd: string | Нет | Пароль отправителя |
| properties | property |  | Массив свойств, можно добавить дополнительные свойства запроса (по согласованию с ШЭП и системой получателя |
| Key | xsd: string | Да | Ключ свойства |
| Value | xsd: string | Да | Значение свойства |
| messageData | messageData | Да | Объект передачи данных |
| Data | xsd: Anytype | Да | Объект данные сообщения (формат определяется системой получателя сообщения) |

Ответ об ошибке (SendMessagefault) представляет собой массив элементов со следующими полями:

**Таблица 16** Формат данных SendMessagefault

|  |  |  |  |
| --- | --- | --- | --- |
| **Поле** | **Тип** | **Обязанность** | **Описание** |
| ErrorInfo | ErrorInfo |  | Информация об ошибке |
| errorCode | xsd: string | Да | Код ошибки |
| errorData | xsd: string | Да | Дополнительное описание ошибки |
| errorDate | xsd: dateTime | Да | Дата ошибки |
| subError | ErrorInfo | Нет | Дочерняя ошибка |
| sessionId | guid | Нет | Идентификатор сессии, в которой произошла ошибка |

1.2. Интерфейс для реализации сервиса на стороне пользователей ШЭП, ВШЭП для работы с асинхронным каналом.

Сервис реализуется как на стороне провайдера сервиса, так и на стороне использующей сервис. Сервис реализуют в случае необходимости доставки ШЭП сообщений методом вызова сервиса получателя сообщения (PUSH).

**Метод приема сообщений: (SendMessage)**

**Запрос на предоставление cообщения (SendMessageRequest)** содержит следующие поля:

**Таблица 17** Формат данных SendMessageRequest

|  |  |  |  |
| --- | --- | --- | --- |
| **Поле** | **Тип** | **Обязанность** | **Описание** |
| request | Async SendMessageRequest | Да |  |
| messageInfo | Async SendMessageInfo | Да | Мета данные сообщения |
| messageId | xsd: string | Да | Идентификатор сообщения.Генерируется ШЭП. В случае отправки сообщения на ШЭП данное поле должно быть пустым. В случае передачи сообщения получателю номер будет проставлен ШЭП. |
| correlationId | xsd: string | Нет | Идентификатор цепочки сообщений. Генерируется ШЭП. В случае отправки сообщения типа REQUEST на ШЭП данное поле должно быть пустым. При отправке сообщений других типов на ШЭП, данное поле ДОЛЖНО БЫТЬ ЗАПОЛНЕНО. В случае передачи сообщения получателю номер будет проставлен ШЭП. |
| serviceId | xsd: string | Да | Идентификатор взаимодействия. По реестру сервисов ШЭП. |
| messageType | xsd: string | Да | Тип сообщения:REQUEST - первое сообщения взаимодействия |
| routeId | xsd: string | Нет | Идентификатор маршрута сообщения (если есть необходимость в дополнительной маршрутизации, идентификатор по реестру, заполняется системой отправителя) |
| messageDate | xsd: dateTime | Да | Дата создания сообщения |
| sessionId | guid | Нет | Идентификатор сессии ШЭП. Заполняется на ШЭП, отправителю заполнять не надо. |
| sender | SenderInfo | Да | Объект информация об отправителе (заполняется отправителем) |
| senderId | xsd: string | Да | Идентификатор отправителя (системы отправителя) |
| password | xsd: string | Нет | Пароль отправителя |
| properties | Property | Нет | Массив дополнительных свойств сообщения |
| key | xsd: int | Да | Ключ свойства |
| value | xsd: int | Да | Значение свойства |
| messageData | messageData | Да | Объект передачи данных |
| data | xsd: Anytype | Да | Объект данные сообщения (формат определяется системой получателя сообщения) |

**Ответ ШЭП на сообщение (sendMessageResponse)** представляет собой массив элементов со следующими полями:

**Таблица 18** Формат данных SendMessageResponse

|  |  |  |  |
| --- | --- | --- | --- |
| **Поле** | **Тип** | **Обязанность** | **Описание** |
| response | Async SendMessageResponse | Да | Ответ |
| messageId | xsd: string | Да | Идентификатор сообщения |
| correlationId | xsd: string | Да | Идентификатор цепочки сообщения |
| responseDate | xsd: dateTime | Да | Дата ответа |
| sessionId | guid | Нет | Идентификатор сессии ШЭП |

**Ответ об ошибке (SendMessageFault)** представляет собой массив элементов со следующими полями:

**Таблица 19** Формат данных SendMessageFault

|  |  |  |  |
| --- | --- | --- | --- |
| **Поле** | **Тип** | **Обязанность** | **Описание** |
| ErrorInfo | ErrorInfo |  | Информация об ошибке |
| errorCode | xsd: string | Да | Код ошибки |
| errorData | xsd: string | Да | Дополнительное описание ошибки |
| errorDate | xsd: dateTime | Да | Дата ошибки |
| subError | ErrorInfo | Нет | Дочерняя ошибка |
| sessionId | guid | Нет | Идентификатор сессии в которой произошла ошибка |

**Метод приема уведомлений об изменении статуса сообщения в ШЭП** (ChangeMessageStatusNotification)

Запрос уведомления об изменении статуса сообщения (ChangeMessageStatusNotificationRequest) представляет собой массив элементов со следующими полями:

**Таблица 20** Формат данных ChangeMessageStatusNotificationRequest

|  |  |  |  |
| --- | --- | --- | --- |
| **Поле** | **Тип** | **Обязанность** | **Описание** |
| request | Async ChangeMessageStatus NotificationRequest | Да |  |
| notification | ChangeStatus Notification | Да | Уведомления о статусе доставки сообщения |
| notificationid | xsd: string | Да | Идентификатор уведомления |
| messageId | xsd: string | Да | Идентификатор сообщения |
| notificationDate | xsd: dateTime | Да | Дата создания уведомления |
| messageState |  messageState  | Да | Состояние сообщения |
| Status | messageStatusinfo | Да | Статус доставки (приема сообщения) |
| statusCode | xsd: string | Да | Код статуса |
| statusMessage | xsd: string | Да | Сообщения статуса |
| statusDate | xsd: dateTime | Да  | Идентификатор маршрута сообщения (если есть необходимость в дополнительной маршрутизации, идентификатор по реестру, заполняется системой отправителя) |
| error |  | Нет | Информация об ошибке |
| errorCode | xsd: string | Да | Код ошибки |
| errorMessage | xsd: string | Да | Сообщение ошибки |
| errorData | xsd: string | Да | Дополнительное описание ошибки |
| errorDate | xsd: dateTime | Да | Дата ошибки |
| subError | xsd: string | Нет | Дочерняя ошибка |
| sessionId | guid | Нет | Идентификатор сессии в которой произошла ошибка |
| requestdate | xsd: dateTime | Да | Дата запроса |
| sessionid | guid | Нет | Идентификатор сессии |

Ответ о принятии уведомления (changeMassageStatusNotificationResponse) представляет собой массив элементов со следующими полями:

**Таблица 21** Формат данных ChangeMessageStatusNotificationResponse

|  |  |  |  |
| --- | --- | --- | --- |
| **Поле** | **Тип** | **Обязанность** | **Описание** |
| response | Async ChangeMessageStatus NotificationResponse | Да | Ответ |
| responseDate | xsd: dateTime | Да | Дата ответа |
| sessionid | guid | Да | Идентификатор сессии (указанное в запросе) |

Ответ об ошибке (sendMessageFault) представляет собой массив элементов со следующими полями:

**Таблица 22** Формат данных SendMessageFault

|  |  |  |  |
| --- | --- | --- | --- |
| **Поле** | **Тип** | **Обязанность** | **Описание** |
| ErrorInfo | ErrorInfo |  | Информация об ошибке |
| errorCode | xsd: string | Да | Код ошибки |
| errorData | xsd: string | Да | Дополнительное описание ошибки |
| errorDate | xsd: dateTime | Да | Дата ошибки |
| subError | ErrorInfo | Нет | Дочерняя ошибка |
| sessionId | guid | Нет | Идентификатор сессии в которой произошла ошибка |

**Коды ошибок при взаимодействии с ВШЭП/ШЭП**

**Таблица 23 Коды ошибок асинхронного канала**

ACE001 Сообщение не соответствует формату

ACE002 Неправильный логин или пароль

ACE003 Пользователь не имеет прав на сервис

ACE004 Сообщение REQUEST не прошло логическую проверку

ACE005 Сообщение UPDATE не прошло логическую проверку

ACE006 Сообщение NOTIFICATION не прошло логическую проверку

ACE007 Сообщение RESPONSE не прошло логическую проверку

ACE008 Не существует такой цепочки сообщений

ACE009 Сервис не существует

**Таблица 24 Внутренние ошибки ШЭП, ВШЭП**

ACIE001 Ошибка генерации идентификатора цепочки сообщения, для сообщения REQUEST

ACIE002 Ошибка генерации идентификатор сообщения для REQUEST

ACIE003 Ошибка генерации идентификатора сообщения UPDATE

ACIE004 Ошибка генерации идентификатора сообщения NOTIFICATION

ACIE005 Ошибка генерации идентификатора сообщения RESPONSE

ACIE006 Ошибка сохранения в БД сообщения REQUEST

ACIE007 Ошибка сохранения в БД сообщения UPDATE

ACIE008 Ошибка сохранения в БД сообщения NOTIFICATION

ACIE009 Ошибка сохранения в БД сообщения RESPONSE

ACIE010 Ошибка отправки в очередь сообщения REQUEST

ACIE011 Ошибка отправки в очередь сообщения UPDATE

ACIE012 Ошибка отправки в очередь сообщения NOTIFICATION

ACIE013 Ошибка отправки в очередь сообщения RESPONSE

ACIE014 Ошибка формирования ответа на сообщения REQUEST

ACIE015 Ошибка формирования ответа на сообщения UPDATE

ACIE016 Ошибка формирования ответа на сообщения NOTIFICATION

ACIE017 Ошибка формирования ответа на сообщения RESPONSE

ACIE018 Ошибка отправки ответа на сообщения REQUEST

ACIE019 Ошибка отправки ответа на сообщения UPDATE

ACIE020 Ошибка отправки ответа на сообщения NOTIFICATION

ACIE021 Ошибка отправки ответа на сообщения RESPONSE

# ПРИЛОЖЕНИЕ 2

**Схемы взаимодействия**

**Схема directionCardFiles**

<?xml version='1.0' encoding='UTF-8'?>

 <xs:schema

 xmlns:ns1="http://conclusionFileBase64.persistence.interactive.nat"

 xmlns:xs="http://www.w3.org/2001/XMLSchema"

 targetNamespace="http://directionCardFiles.persistence.interactive.nat"

 version="1.0">

 <xs:import namespace="http://conclusionFileBase64.persistence.interactive.nat"/>

 <xs:complexType name="DirectionCardFiles">

 <xs:annotation>

 <xs:documentation>Карточка заключения</xs:documentation>

 </xs:annotation>

 <xs:sequence>

 <xs:element name="IIN" type="xs:string">

 <xs:annotation>

 <xs:documentation>ИИН</xs:documentation>

 </xs:annotation>

 </xs:element>

 <xs:element name="BIN" type="xs:string">

 <xs:annotation>

 <xs:documentation>БИН</xs:documentation>

 </xs:annotation>

 </xs:element>

 <xs:element name="ConclusionNumber" type="xs:string">

 <xs:annotation>

 <xs:documentation>Номер заключения</xs:documentation>

 </xs:annotation>

 </xs:element>

 <xs:element name="ConclusionDate" type="xs:dateTime">

 <xs:annotation>

 <xs:documentation>Дата заключения</xs:documentation>

 </xs:annotation>

 </xs:element>

 <xs:element name="ConclusionFileBase64" type="ns1:ConclusionFileBase64">

 <xs:annotation>

 <xs:documentation>Окончательная версия ПСД</xs:documentation>

 </xs:annotation>

 </xs:element>

 </xs:sequence>

 </xs:complexType>

</xs:schema>

**Схема declareRequestResponseAsync**

<?xml version='1.0' encoding='UTF-8'?>

<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:tns="http://message.persistence.interactive.nat"

 targetNamespace="http://smartbridge.b10.kz" version="1.0">

 <xs:import namespace="http://message.persistence.interactive.nat"/>

 <xs:element name="sendMessageRequest" type="tns:SendMessageRequest"/>

 <xs:element name="sendMessageResponse" type="xs:string"/>

 <xs:element name="receiveMessageRequest" type="xs:string"/>

 <xs:element name="receiveMessageResponse" type="tns:ConclusionCardResponse"/>

</xs:schema>

**Схема conclusionFileBase64**

<?xml version='1.0' encoding='UTF-8'?>

<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" targetNamespace="http://conclusionFileBase64.persistence.interactive.nat"

 version="1.0">

 <xs:complexType name="ConclusionFileBase64">

 <xs:annotation>

 <xs:documentation>Текст заключения</xs:documentation>

 </xs:annotation>

 <xs:sequence>

 <xs:element name="FileName" type="xs:string">

 <xs:annotation>

 <xs:documentation>Наименование файла</xs:documentation>

 </xs:annotation>

 </xs:element>

 <xs:element name="FileSize" type="xs:integer">

 <xs:annotation>

 <xs:documentation>Размер файла</xs:documentation>

 </xs:annotation>

 </xs:element>

 <xs:element name="FilePart" type="xs:base64Binary">

 <xs:annotation>

 <xs:documentation>Массив</xs:documentation>

 </xs:annotation>

 </xs:element>

 <xs:element name="MD5Hash" type="xs:string">

 <xs:annotation>

 <xs:documentation>MD5 Hash</xs:documentation>

 </xs:annotation>

 </xs:element>

 <xs:element name="FilePartCount" type="xs:string">

 <xs:annotation>

 <xs:documentation>Общее количество частей файла</xs:documentation>

 </xs:annotation>

 </xs:element>

 </xs:sequence>

 </xs:complexType>

</xs:schema>

**Схема message**

<?xml version='1.0' encoding='UTF-8'?>

<xs:schema xmlns:ns1="http://directionCardFiles.persistence.interactive.nat"

 xmlns:xs="http://www.w3.org/2001/XMLSchema" targetNamespace="http://message.persistence.interactive.nat"

 version="1.0">

 <xs:import namespace="http://directionCardFiles.persistence.interactive.nat"/>

 <xs:complexType name="SendMessageRequest">

 <xs:annotation>

 <xs:documentation>

 Запрос на получения файлов по градостроительным и строительным проектам по запросу

 </xs:documentation>

 </xs:annotation>

 <xs:sequence>

 <xs:element name="ConclusionNumber" type="xs:string">

 <xs:annotation>

 <xs:documentation>Номер заключения</xs:documentation>

 </xs:annotation>

 </xs:element>

 <xs:element name="ConclusionDate" type="xs:dateTime">

 <xs:annotation>

 <xs:documentation>Дата заключения</xs:documentation>

 </xs:annotation>

 </xs:element>

 <xs:element name="CustomerAgreementFileName" type="xs:string">

 <xs:annotation>

 <xs:documentation>Наименование файла согласия</xs:documentation>

 </xs:annotation>

 </xs:element>

 <xs:element name="CustomerAgreementFileUrl" type="xs:string">

 <xs:annotation>

 <xs:documentation>Файл согласия</xs:documentation>

 </xs:annotation>

 </xs:element>

 <xs:element name="FilePart" type="xs:int">

 <xs:annotation>

 <xs:documentation>Текст заключения</xs:documentation>

 </xs:annotation>

 </xs:element>

 </xs:sequence>

 </xs:complexType>

 <xs:complexType name="ConclusionCardResponse">

 <xs:annotation>

 <xs:documentation>Сообщение ответа на запрос</xs:documentation>

 </xs:annotation>

 <xs:sequence>

 <xs:element name="correctnessCode" type="xs:unsignedByte">

 <xs:annotation>

 <xs:documentation>

 Корректность: 0 – заключения не существует 1 – заключение существует 2 – заключение аннулировано 3 – доступ запрещён 4 – файл согласия по ссылке не найден 5 – нет АВР по проекту 6 - не подписан авторский договор 7 – архив окончательной версии ПСД отсутствует 8– доступ к ПСД отключен

 </xs:documentation>

 </xs:annotation>

 </xs:element>

 <xs:element name="directionCardFiles" type="ns1:DirectionCardFiles">

 <xs:annotation>

 <xs:documentation>Карточка направления</xs:documentation>

 </xs:annotation>

 </xs:element>

 </xs:sequence>

 </xs:complexType>

</xs:schema>

**Пример запроса request\_async**

<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">

<SOAP-ENV:Header/>

<SOAP-ENV:Body>

<ns3:SendMessage xmlns:ns3="http://bip.bee.kz/AsyncChannel/v10/Types" xmlns="">

<request>

<requestInfo>

<messageId>ccb1010b-8446-4937-913f-c87a717f6809</messageId>

<serviceId>GBDFL\_UniversalServiceSync</serviceId>

<messageDate>2019-12-25T12:48:21.024Z</messageDate>

<sender>

<senderId>smartbridge</senderId>

<password>123</password>

</sender>

<properties>

<key>CONNECTOR\_CLIENT</key>

<value>true</value>

</properties>

</requestInfo>

<requestData>

<ns4:data xmlns:ns4="http://bip.bee.kz/SyncChannel/v10/Interfaces" xmlns:cs="http://message.persistence.interactive.nat" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="cs:SendMessageRequest">

<ConclusionNumber>01-0442/171</ConclusionNumber>

<ConclusionDate>2021-12-29T15:22:16.183+06:00</ConclusionDate>

<CustomerAgreementFileName>Test.pdf</CustomerAgreementFileName>

<CustomerAgreementFileUrl>http://.....3317-6187-4371-bab4-31f92b22b0e8.pdf</CustomerAgreementFileUrl>

<FilePart>1</FilePart>

</ns4:data>

</requestData>

</request>

</ns3:SendMessage>

</SOAP-ENV:Body>

</SOAP-ENV:Envelope>

**Пример ответа response\_async**

<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">

<soap:Header/>

<soap:Body>

<ns2:SendMessageResponse xmlns:ns2="http://bip.bee.kz/AsyncChannel/v10/Types" xmlns:ns3="http://bip.bee.kz/AsyncChannel/v10/Interfaces">

<response>

<responseInfo>

<messageId>dfb3b761-d350-4aeb-869f-987346993</messageId>

<correlationId>1</correlationId>

<responseDate>2019-07-18T15:26:49.486+06:00</responseDate>

<status>

<code>SCSS001</code>

<message>Message has been processed successfully</message>

</status>

<sessionId>1</sessionId>

</responseInfo>

<responseData>

<data xmlns:cs="http://message.persistence.interactive.nat" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="cs:ConclusionCardResponse">

<correctnessCode>1</correctnessCode>

<directionCardFiles>

<IIN>222233333333</IIN>

<BIN>012345678921</BIN>

<ConclusionNumber>01-0442/171</ConclusionNumber>

<ConclusionDate>2021-12-29T00:00:00</ConclusionDate>

<ConclusionFileBase64>

<FileName>01-0442/171.zip</FileName>

<FileSize>854423</FileSize>

<FilePart>ODQxMDExMTUxMTY=</FilePart>

<MD5Hash>/LS7W6G6I5BIni4ezT0dag==</MD5Hash>

<FilePartCount>3</FilePartCount>

</ConclusionFileBase64>

</directionCardFiles>

<Signature xmlns="http://www.w3.org/2000/09/xmldsig#" xmlns:ds="http://www.w3.org/2000/09/xmldsig#" Id="1">

<SignedInfo>

<CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>

<SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>

<Reference URI="">

<Transforms>

<Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>

<Transform Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315#WithComments"/>

</Transforms>

<DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>

<DigestValue>IGAA+NH9sDRku7GSjyHPyTTBDMUtl/R2ojRKsVV224w=</DigestValue>

</Reference>

</SignedInfo>

<SignatureValue>hm500oej9PSQeUJbzjj95iGrswBmaNca0FzlCdAEQQ0+i/dnn85yzskO+w2PcZmw 8opS0Fu76WGt1W8k6tYVmCCMQzJIuCC5g3t8pZKXGLAKIbXy4Yt2LXPIC9uyL+uy WxbUwMaJIaPWk2bQWmm7P/Jc7P8HD8spD4oLfxLxqnDBIc2LxoALGvMTpWFxB5ng ZrcjPv+Bf+OvQEd+cE5REbYYg8h+GLGAGlsLgC28tFIP/5J0jFyJQP19bIj0SCxQ WhZ64Gisfu28Non48aPiOyI+As+jGbGh/8+jpF6nObOYLxFY2kb83bhoz+/5dqEl NaNVCGqGER14sZ+XsJDhVw== </SignatureValue>

<KeyInfo>

<X509Data>

<X509Certificate>MIIGtzCCBJ+gAwIBAgIUIKeF5vWQ== </X509Certificate>

</X509Data>

</KeyInfo>

</Signature>

</data>

</responseData>

</response>

</ns2:SendMessageResponse>

</soap:Body>

</soap:Envelope>

# ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

| Изм. | Номера листов (страниц) | Всего листов (страниц) в докум. | № докум. | Входящий № сопроводительного докум. и дата | Подп. | Дата |
| --- | --- | --- | --- | --- | --- | --- |
| Измененных | Замененных | новых | Аннулированных |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |

# ЛИСТ СОГЛАСОВАНИЯ

**Согласовано**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Организация** | **Должность исполнителя** | **Фамилия И.О.** | **Подпись** | **Дата** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |