**Инструкция**

**по подаче заявки на публикацию сервиса (для ИС вне ЕТС)**

Настоящая инструкция по подаче заявки на публикацию сервиса на ШЭП/ВШЭП предназначена для владельцев информационных систем (Владельцев сервиса), находящихся в сети Интернет.

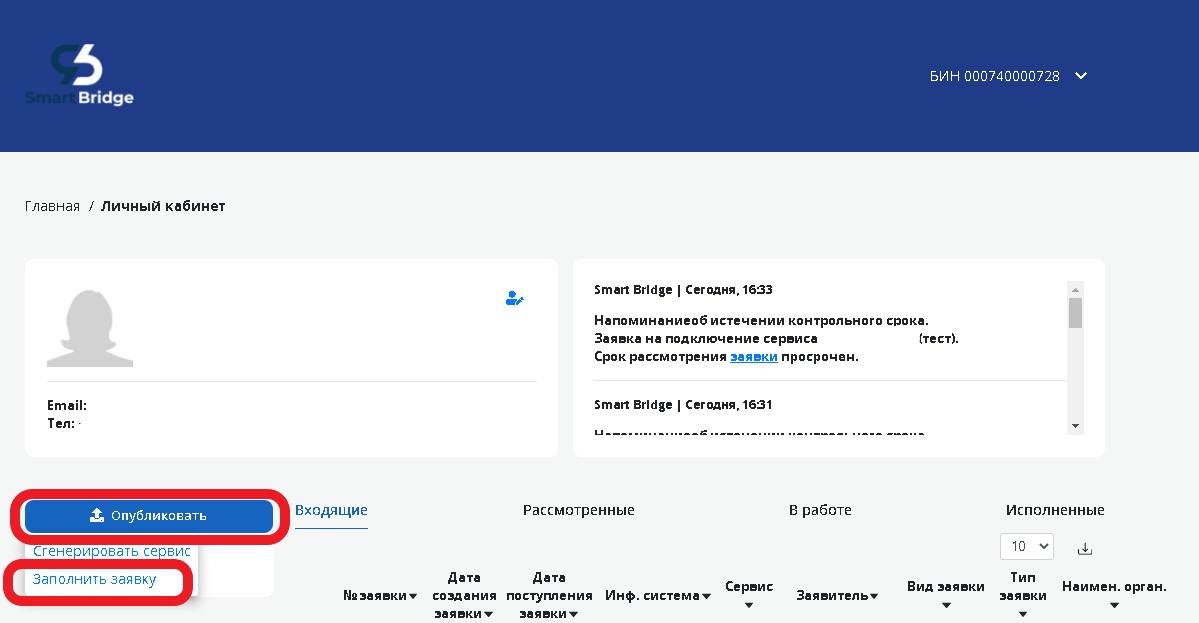
На портале Smart Bridge предусмотрена возможность подачи заявки на публикацию сервиса с указанием Клиента и без указания Клиента.

* В случае оставления поля «Клиент сервиса» пустым заявка после подписания поступает в АО «НИТ». АО «НИТ» проводятся работы по публикации сервиса одновременно в тестовой и в промышленной среде ШЭП/ВШЭП, также публикуется паспорт сервиса на портале Smart Bridge. После чего другие организации могут подавать заявки на подключение к данному сервису. Тестирование и подписание актов тестирования будет проводиться согласно поданным заявкам на подключение.

В случае заполнения поля «Клиент сервиса» заявка поступает на рассмотрение в организацию, указанную в заявке Клиентом. Клиент должен заполнить в заявке вкладку «Заявка на подключение». Затем заявка поступает в АО «НИТ». АО «НИТ» проводятся работы по публикации сервиса в тестовой среде ШЭП/ВШЭП и подключению к нему Клиента. Сетевые инженеры АО «НИТ» проверяют доступ по сети, и в случае организации нового VPN-соединения подготавливают и высылают заявителю PSK-ключ для настройки VPN-туннеля на своей стороне.

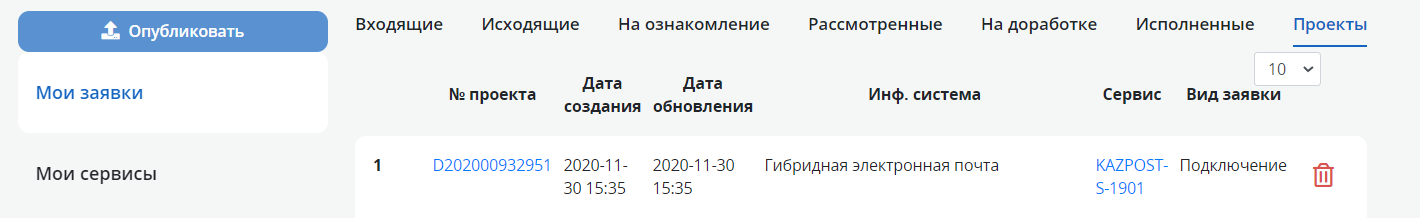
После Владелец и Клиент сервиса проводят тестирование, в рамках текущей заявки подписывают акт тестирования (инициирует Владелец сервиса). Далее АО «НИТ» на основании акта тестирования и наличия сообщений на тестовом ШЭП/ВШЭП публикует сервис в промышленном ШЭП/ВШЭП и подключает к нему Клиента, также публикуется паспорт сервиса на портале Smart Bridge.

Для подачи заявки на публикацию сервиса на ШЭП/ВШЭП необходимо на главной странице либо в Личном кабинете нажать на кнопку «Опубликовать сервис»:



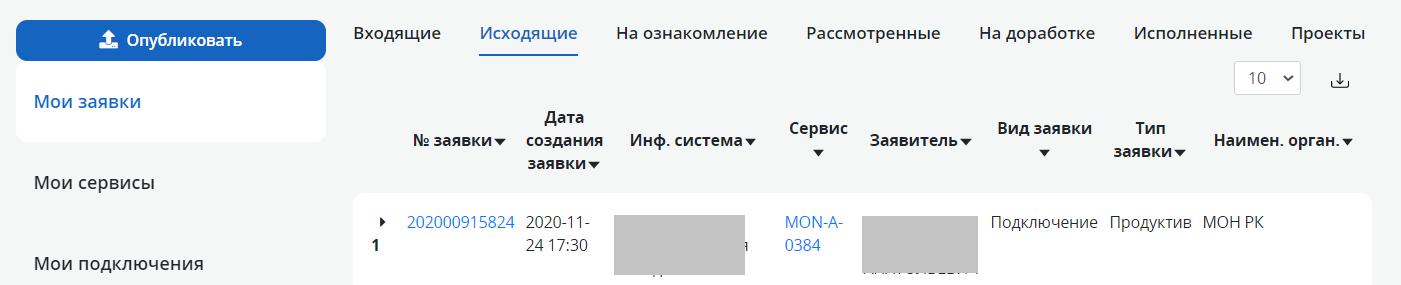
В открывшейся форме заявки на публикацию следует заполнить обязательные поля, отмеченные красной звездочкой «\*». Ниже в настоящей инструкции приведены пояснения к заполнению полей заявки.

При частичном заполнении заявки возможно сохранить заявку (кнопка «Сохранить»). Черновик (проект) заявки сохранится в папке «Проекты» вкладки «Мои заявки» в личном кабинете. Проект заявки позже можно заполнить и подписать ЭЦП. **При этом проект заявки отображается только для сотрудника, инициировавшего ее.** Проект заявки можно удалить с помощью кнопки в виде корзины:



После заполнения всех обязательных полей становится активной кнопка «Далее» для перехода на страницу проверки введенных данных. В случае корректного заполнения нажать на кнопку «Подписать ЭЦП».

После подписания заявка переместится в папку «Исходящие» вкладки «Мои заявки»:

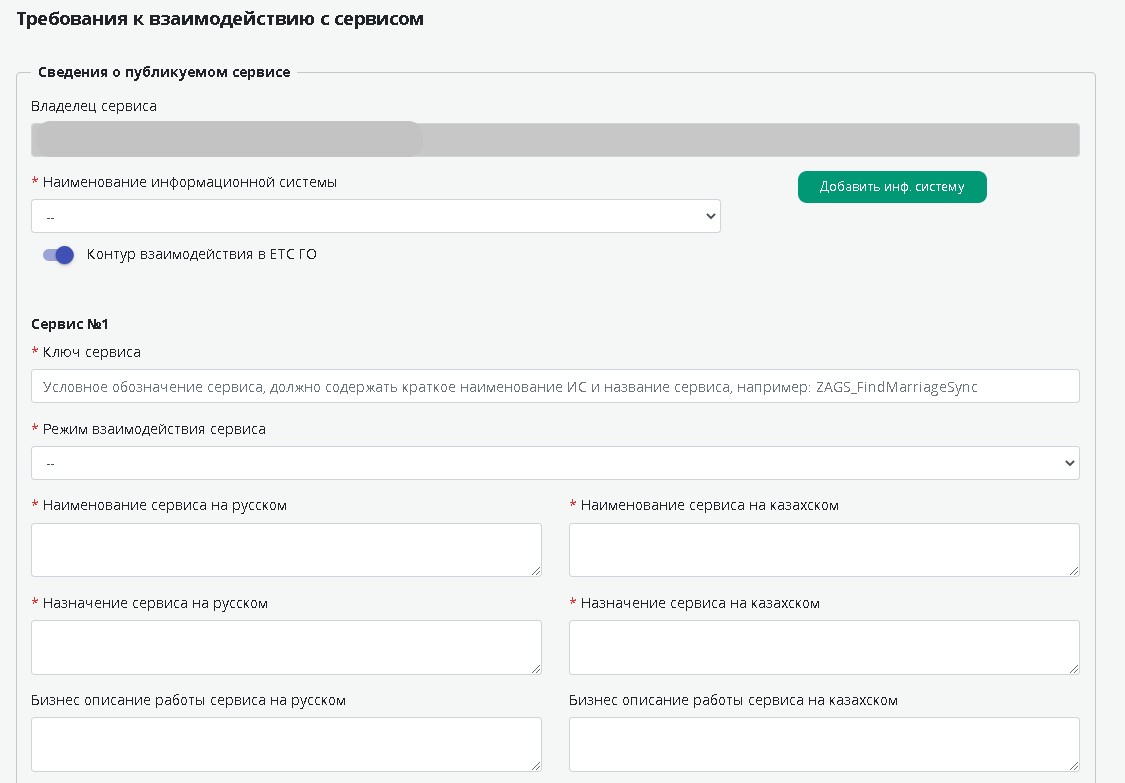


Подписанные заявки отображаются в личном кабинете организации всем сотрудникам, которые имеют ЭЦП сотрудника юридического лица.

**! На портале Smart Bridge имеется возможность самостоятельного отслеживания заявки, подробнее описано в соответствующей инструкции раздела Помощь портала.**

Пояснения к заполнению полей заявки

Поля страницы «Требования к взаимодействию с сервисом»



*«Наименование информационной системы»* – в данном поле необходимо выбрать из выпадающего списка информационную систему, которая предоставляет публикуемый веб-сервис.

При отсутствии информационной системы в выпадающем списке необходимо добавить ее с помощью кнопки «Добавить инф.систему». Процесс добавления информационной системы описан подробнее в соответствующей инструкции раздела Помощь портала Smart Bridge.

В случае возникновения ошибки следует направить текст, которым заполняются поля в окне добавления системы, а также БИН, который отображается в личном кабинете Smart Bridge, на почту поддержки sb.egov@nitec.kz для добавления системы вручную.

*«Контур взаимодействия»* – указывается контур взаимодействия системы вне ЕТС, необходимо передвинуть переключатель «Контур взаимодействия» в неактивное положение:



*«Ключ сервиса»* – необходимо указать условное наименование сервиса:

• заполнять латинскими буквами

• в названии необходимо включить краткое название ИС и краткое название сервиса.

**! Ключ сервиса – это уникальный идентификатор сервиса на ШЭП/ВШЭП, он не должен совпадать с ключами каких-либо иных сервисов вне зависимости от информационной системы или организации-Владельца сервиса.**

*«Режим взаимодействия сервиса»* – следует выбрать из списка: «Синхронный» или «Асинхронный» режим.

Синхронный - запрос с быстрым ответом электронного сервиса.

Асинхронный - запрос с отложенным ответом.

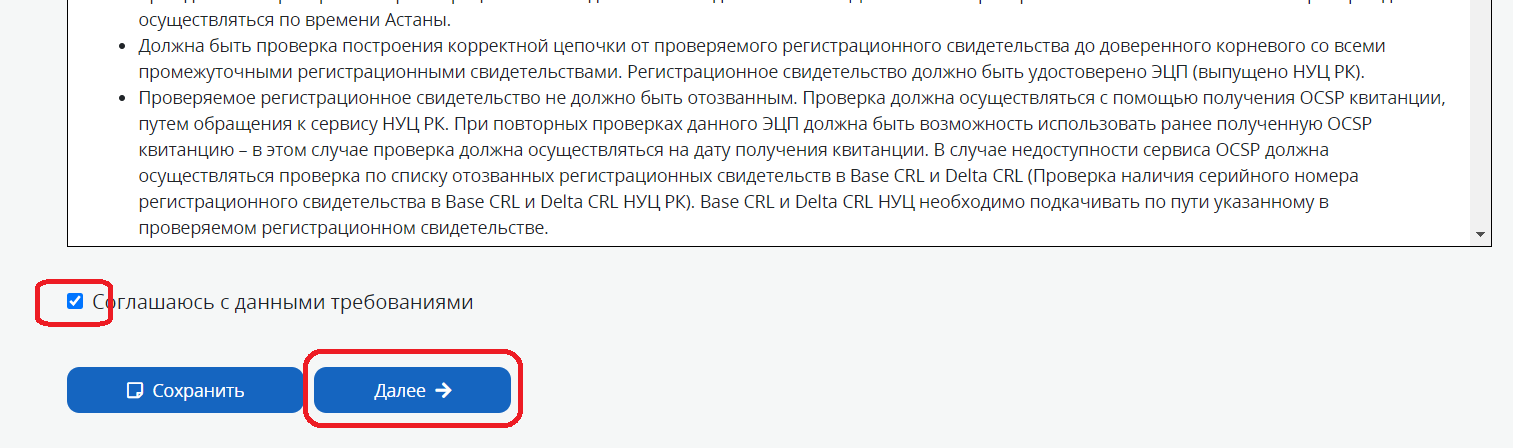
*«Наименование сервиса»* – необходимо указать полное наименование электронного сервиса, не допускаются сокращения в названии, а также использование аббревиатур. Например, сервис передачи регистрационных сведений юридического лица.

*«Назначение сервиса»* – в указанном поле следует указать развернутое, исчерпывающее описание назначения электронного сервиса. Например, сервис предназначен для передачи регистрационных сведений юридического лица.

*«Бизнес описание работы сервиса»* – необходимо указать бизнес описание работы сервиса, например, «Данный сервис предоставляет данные в рамках оказания услуги «Выдача электронного свидетельства о рождении» на ПЭП».

В случае необходимости возможно изменить значения полей «Требований по производительности и надежности».

Далее следует согласиться с требованиями ШЭП, нажать кнопку «Далее» для перехода на следующую страницу «Заявка на публикацию сервиса» (при этом заявка автоматически сохранится в папке Проекты вкладки Мои сервисы Личного кабинета Smart Bridge):



Поля страницы «Заявка на публикацию сервиса»

*«Должностное лицо, ответственное за эксплуатацию»* – это данные контактного лица для организации взаимодействия с администраторами и разработчиками сервиса: ФИО, должность, контактный телефон, электронная почта в формате.

Шаблон заполнения:

Фамилия И.О.

Должность

Организация

Тел.: +7 (7172) 11-22-33, +7 (700) 123-12-12

E-mail:

*«Корневая категория сервиса»* – выбрать категорию выбрать из выпадающего списка, которая наиболее подходит для публикуемого сервиса.

*«Контактные данные разработчика сервиса»* – указать контактное лицо, напрямую отвечающее за разработку (техническую поддержку) сервиса, с кем можно контактировать для уточнения технических деталей функционирования сервиса или устранения инцидентов при его неработоспособности (технический специалист): ФИО, должность, контактный телефон, электронная почта.

Шаблон заполнения:

Фамилия И.О.

Должность

Организация

Тел.: +7 (7172) 11-22-33, +7 (700) 123-12-12

E-mail:

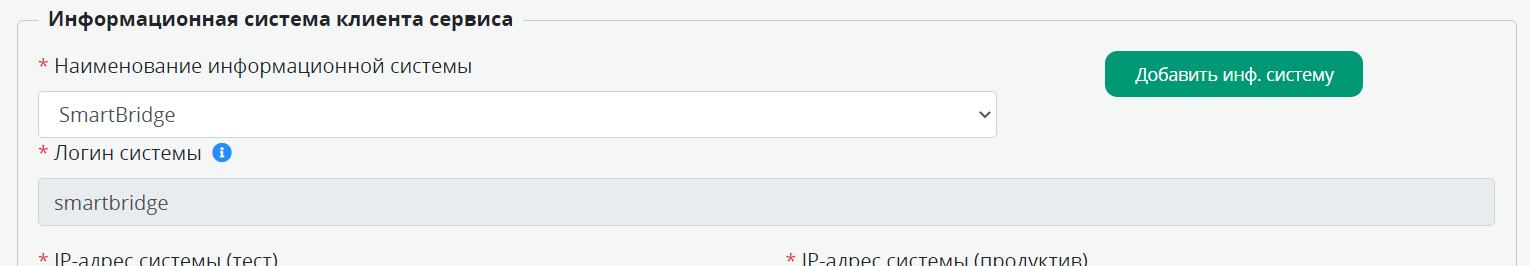
*«Логин системы»* – это логин системы, под которым она будет заведена на ВШЭП, необходимо придумать его и ввести в поле (также сохранить у себя для информации). Логин системы должен быть идентичным в тестовой и промышленной среде ВШЭП. Логин должен содержать как минимум 3 символа, допускается использование только строчных и прописных букв латинского алфавита и цифр.

*«Пароль (тест)»* – это пароль системы для ее авторизации в тестовой среде ВШЭП, необходимо придумать его и ввести в поле (также сохранить у себя для информации). Пароль должен содержать как минимум 8 символов.

*«Пароль (продуктив)»* – это пароль системы для ее авторизации в промышленной среде ВШЭП, необходимо придумать его и ввести в поле (также сохранить у себя для информации). Пароль должен содержать как минимум 8 символов.

**! Если ранее до внедрения портала «Smart Bridge» уже публиковались веб-сервисы данной системы на ВШЭП либо проводилось ее подключение к веб-сервисам на ВШЭП, то у нее уже имеются авторизационные данные, их необходимо ввести в полях логина и паролей системы.**

Следует отметить, что после проведения работ на тестовой среде ШЭП по данной заявке логин системы сохраняется на портале «Smart Bridge». Логин будет отображаться при выборе системы как нередактируемое поле, а поля паролей отображаться не будут:



*«IP-адрес системы (тест)»* – это IP-адрес системы в тестовой среде. Необходимо указать **публичный (белый) IP-адрес**, это должен быть IP-адрес сервера тестовой системы, с которого будут отправляться сообщения типа «запрос».

*«IP-адрес системы (продуктив)»* – это IP-адрес системы в тестовой среде. Необходимо указать **публичный (белый) IP-адрес**, это должен быть IP-адрес сервера промышленной системы, с которого будут отправляться сообщения типа «запрос».

**! В соответствии с требованиями информационной безопасности контуры взаимодействия тестовой и промышленной сред системы должны совпадать (и тестовая и промышленная системы должны располагаться в одном контуре). В противном случае заявка будет отправлена АО «НИТ» на доработку.**

*«Порт системы (тест)»* – это порт, по которому для Клиента будет организовываться доступ к сервису по сети в тестовой среде ВШЭП. Это поле заполняется на усмотрение разработчика веб-сервиса подключения.

«Порт системы (продуктив)» – это порт, по которому для Клиента будет организовываться доступ к сервису по сети в промышленной среде ВШЭП. Это поле заполняется на усмотрение разработчика веб-сервиса подключения.

При наличии нескольких портов возможно указание их через запятую без символа пробела (пример: 80,8080,8090).

*«Протокол (тест)»* – это протокол, по которому для Клиента будет организовываться доступ к сервису по сети в тестовой среде ШЭП/ВШЭП. Это поле заполняется на усмотрение разработчика веб-сервиса подключения, чаще используется TCP протокол.

*«Протокол (продуктив)»* – это протокол, по которому для Клиента будет организовываться доступ к сервису по сети в промышленной среде ШЭП/ВШЭП. Это поле заполняется на усмотрение разработчика веб-сервиса подключения, обычно используется TCP протокол.

*«Прикрепите сертификат открытого ключа транспортной ЭЦП системы (.cer; .crt)»* – файл с расширением .cer или .crt, скачанный на сайте Национального удостоверяющего центра РК pki.gov.kz.

Если у ИС отсутствует транспортная подпись, то в качестве транспортной может быть выбрана ЭЦП первого руководителя или любого сотрудника с правом подписи документов. Необходимо из ключа GOST для подписания извлечь открытую (публичную) часть на сайте НУЦ РК. Подробнее процесс извлечения открытой части транспортной ЭЦП описан в соответствующей инструкции раздела Помощь портала Smart Bridge.

*«Прикрепите акт по результатам испытаний на соответствие требованиям информационной безопасности (.doc, .docx, .pdf)»* – не обязательное поле. Обязательно для государственных ИС, а также негосударственных ИС, предназначенных для формирования государственных электронных информационных ресурсов, осуществления государственных функций и оказания государственных услуг (согласно подпункту 6 пункта 2 статьи 49 ЗРК от 24 ноября 2015 года № 418-V ЗРК «Об информатизации»).

*«Имеется VPN-туннель для данной системы?»* – Переключатель «нет»/«да». В случае отсутствия VPN-туннеля отображается ссылка на «Технические условия для организации VPN соединения».

***Блок полей Данные VPN-туннеля.*** Большая часть полей данного блока заполняется системой автоматически либо предоставляются на выбор возможные значения в выпадающих списках, обязательных для заполнения два поля (Информация о шлюзе VPN, Публичный Peer IP-адрес). Данные для заполнения полей предоставляет специалист, обладающий знаниями сетевой инфраструктуры.

*«Информация о шлюзе VPN»* – **обязательное поле**, это модель оборудования, где будет организован VPN-туннель. Например, CISCO ACA123.

*«Режим туннеля»* – заполняется автоматически значением «TUNNEL».

*«Публичный Peer IP-адрес»* – **обязательное поле**, это публичный (белый) IP-адрес устройства, на котором будет организован VPN-туннель.

*«Фаза 1: Метод аутентификации»* – заполняется автоматически значением «PSK(Pre-shared key)».

*«Фаза 1: Частный общий ключ»* – сложный пароль для получения доступа к VPN-туннелю. Способ его передачи указывается по умолчанию, заполняется автоматически значением «Нарочно».

*«Фаза 1: Тип криптографии»* – выбрать из выпадающего списка (IKEv2 (*рекомендуемый*) или IKEv1)

*«Фаза 1: Протокол Деффи-Хеллмана»* – заполняется автоматически согласно выбранному типу криптографии: IKEv1 - Group 5 или IKEv2 - Group 14.

*«Фаза 1: Криптографический алгоритм»* – алгоритм преобразования данных, выбрать из выпадающего списка (АES-256 (*рекомендуемый*), 3DES, AES-GMAC-256, AES, AES-GCM-192, AES-GMAC-192, AES-GCM-256, AES-GCM, AES-GMAC, AES-192).

*«Фаза 1: Алгоритм хеширования»* – алгоритм хэширования данных, выбрать из выпадающего списка (SHA256 (*рекомендуемый*), SHA384, SHA512, SHA-1).

*«Фаза 1: Срок действия (для пересмотра построения туннеля)»* – заполняется автоматически значением «default». Это время жизни ключа сеанса – сколько времени должно пройти до смены ключа. Значение по умолчанию равно 86400 секунд.

*«Фаза 2: Инкапсуляция»* – заполняется автоматически значением «ESP (Encapsulating Security Payload)».

*«Фаза 2: Криптографический алгоритм»* – алгоритм преобразования данных, выбрать из выпадающего списка (АES-256 (*рекомендуемый*), 3DES, AES-GMAC-256, AES, AES-GCM-192, AES-GMAC-192, AES-GCM-256, AES-GCM, AES-GMAC, AES-192).

*«Фаза 2: Метод алгоритма»* – алгоритм хэширования данных, выбрать из выпадающего списка (SHA256 (*рекомендуемый*), SHA384, SHA512, SHA-1).

*«Фаза 2: Группа совершенной прямой секретности»* – заполняется автоматически согласно выбранному типу криптографии: IKEv1 - Group 5 или IKEv2 - Group 14.

*«Фаза 2: Срок действия (для пересмотра построения туннеля)»* – заполняется автоматически значением «default». Это время жизни ключа сеанса – сколько времени должно пройти до смены ключа. Значение по умолчанию равно 86400 секунд.

*«Фаза 2: Величина в Kб (для пересмотра построения туннеля)»* – заполняется автоматически значением «default».

***Блок полей «Электронные сервисы»***.

*«Наименование сервиса»* – наименование сервиса в его паспорте, поле для информации заявителю, заполняется автоматически.

*«Ключ сервиса»* – ключ сервиса на ШЭП/ВШЭП, поле для информации заявителю, заполняется автоматически.

*«Режим взаимодействия сервиса»* – синхронный или асинхронный, поле для информации заявителю, заполняется автоматически.

*«Опубликовать сервис на ШЭП»* – переключатель «нет»/«да». В случае если клиенты публикуемого сервиса находятся в ЕТС, необходима публикация на ШЭП.

*«Сервис предоставляет персональные данные»* – признак использования персональных данных граждан при передаче данных сервисом. Поле для информации заявителю, заполняется автоматически

*«Предусмотрена отправка SMS гражданам для получения разрешения на предоставление их персональных данных»* – признак использования механизма отправки SMS при отправке запроса на получение разрешения на предоставление персональных данных. Поле для информации заявителю, заполняется автоматически

*«Режим отправки сообщений»* – выберите метод PULL или PUSH.

Метод PULL – система Клиента самостоятельно извлекает из ШЭП/ВШЭП адресованные ей сообщения.

Метод PUSH – ШЭП/ВШЭП отправляет ответы на запросы системе Клиента.

В случае выбора метода отправки сообщений PUSH, необходимо заполнить следующие поля:

*«Признак наличия маршрутизации сообщений»* – переключатель «нет»/«да». Указывается «да», если по одному сервису есть несколько адресов доставки. В случае наличия признака маршрутизации сообщений необходимо заполнить поле:

«*Ключ маршрута*» – условное обозначение ключа маршрута для дальнейшей идентификации. Заполнять на латинице с использованием цифр.

*«Наименование URL сервиса, принимающего ответы (тест)»* –заполняется автоматически.

*«URL сервиса, принимающего ответы (тест)»* – необходимо указать URL системы, принимающей ответы в тестовой среде.

*«Наименование URL сервиса, принимающего ответы (прод)»* –заполняется автоматически.

*«URL сервиса, принимающего ответы (прод)»* – необходимо указать URL системы, принимающей ответы в промышленной среде.

В случае наличия нескольких адресов доставки по одному сервису необходимо нажать кнопку и заполнить отобразившиеся поля.

*«Наличие авторизации на стороне сервиса»* – переключатель «нет»/«да». В случае наличия авторизации на стороне сервиса необходимо заполнить поля:

*«Метод авторизации»* – необходимо выбрать«Basic» или «Digest» авторизация;

*«Логин»* – следует указать логин для авторизации ИС;

*«Пароль»* – следует указать пароль для авторизации ИС.

«*Тип безопасности*» – тип безопасности, который будет использоваться при передаче данных, выбрать «По логину и паролю» или «Транспортная подпись ГОСТ».

«*Необходимость получения уведомления ИС-отправителей сообщений об изменении статусов сообщений от ШЭП*» – переключатель «нет»/«да».

«*Необходимость получения дополнительного уведомления о доставке от ШЭП*» – переключатель «нет»/«да». Указать «да» в случае необходимости получения от ШЭП уведомлений о доставке запросов системы Клиента в систему Владельца сервиса.

«*Прикрепите SSL сертификат*» – прикрепите открытую часть сертификата безопасности (ключа GOST), файл с расширением .cer или .crt.