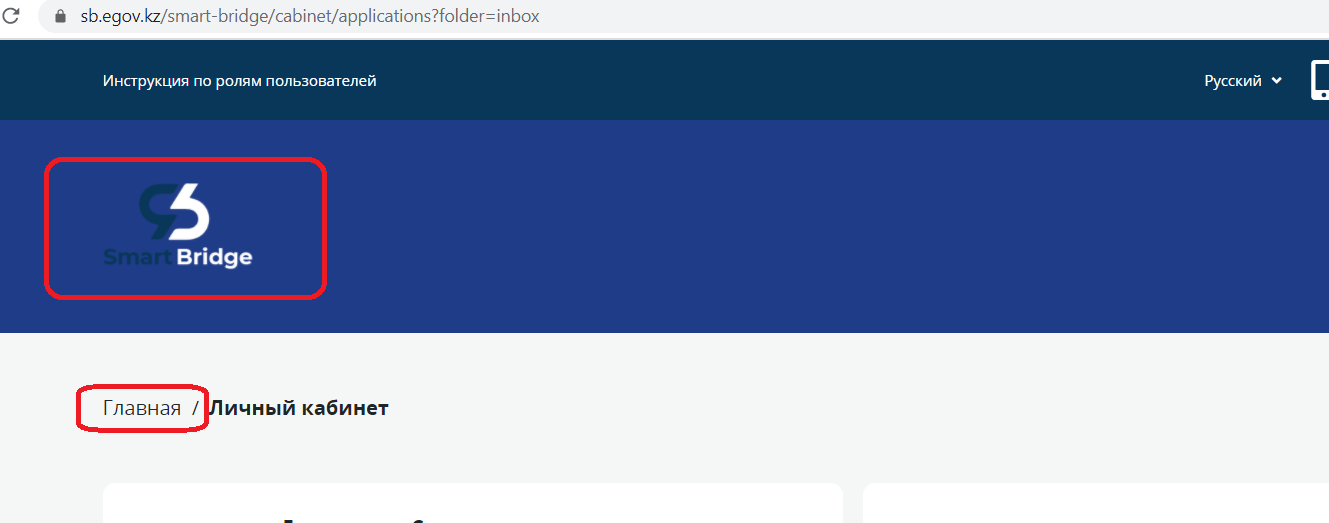
**Инструкция**

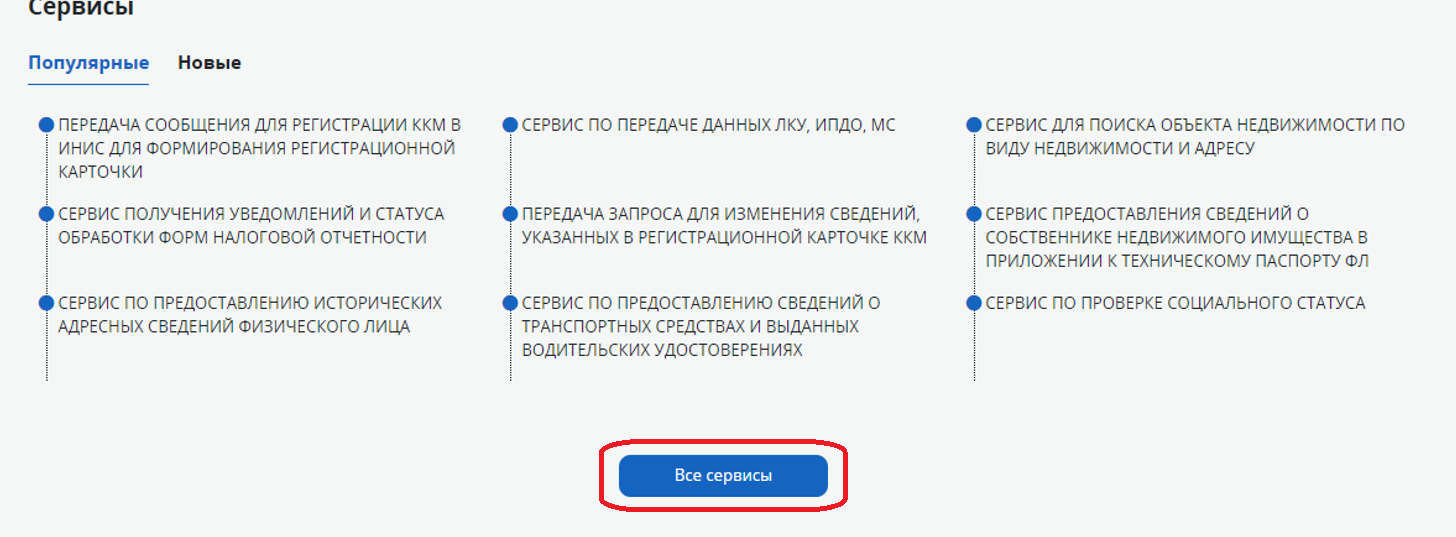
**по подаче заявки на подключение к сервису (для ИС вне ЕТС)**

Настоящая инструкция по подаче заявки на подключение к сервису предназначена для владельцев информационных систем (Клиентов сервиса), находящихся в сети Интернет.

Для подачи заявки на подключение к сервису необходимо найти его паспорт в Каталоге сервисов. Для этого следует открыть Главную страницу портала нажатием на кнопку «Главная» или иконку портала в левом верхнем углу:

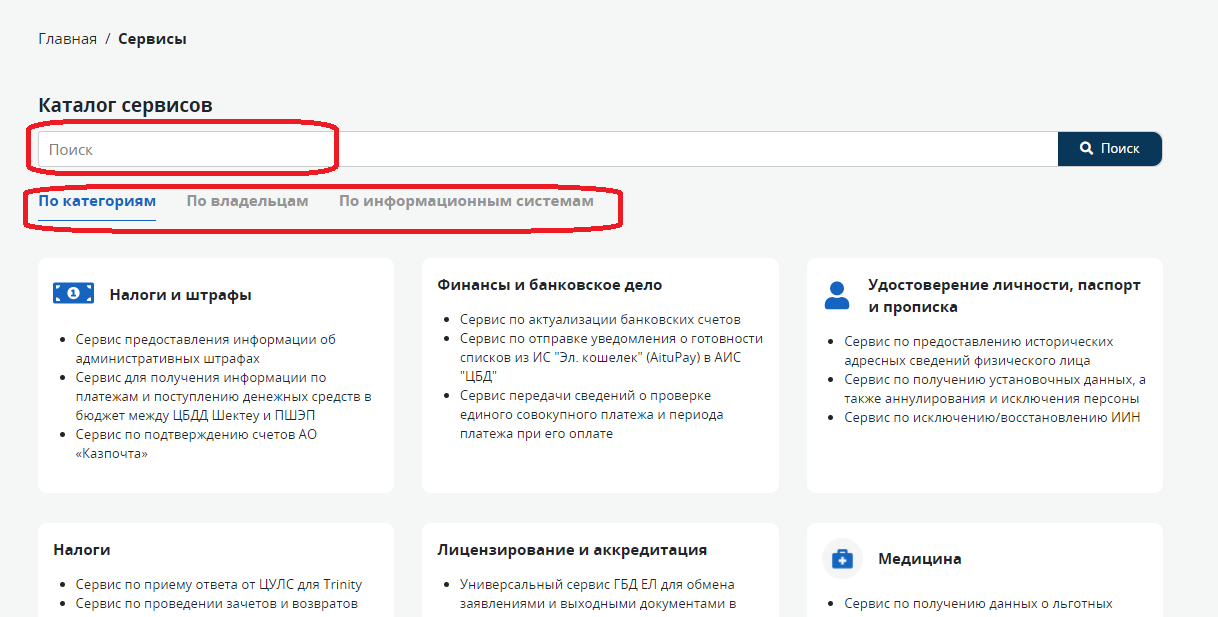


На Главной странице с помощью кнопки «Все сервисы» перейти в Каталог сервисов:

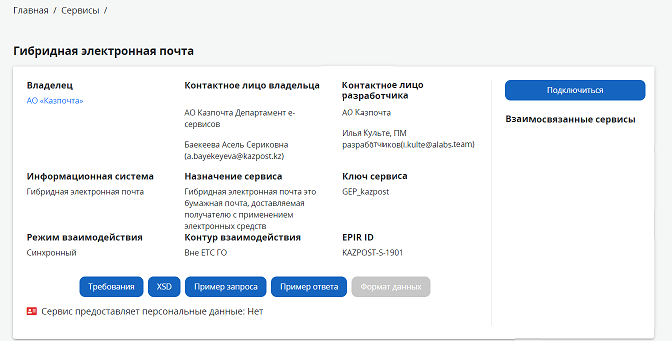


В Каталоге сервисов следует найти паспорт нужного сервиса интеграции. Паспорт сервиса можно найти путем ввода в строку поиска слов из наименования/назначения сервиса или ключа сервиса (ключ сервиса – это уникальный идентификатор, под которым веб-сервис опубликован на ШЭП).

Также возможен поиск в Каталоге сервисов по категориям, по Владельцам и по информационным системам сервисов:



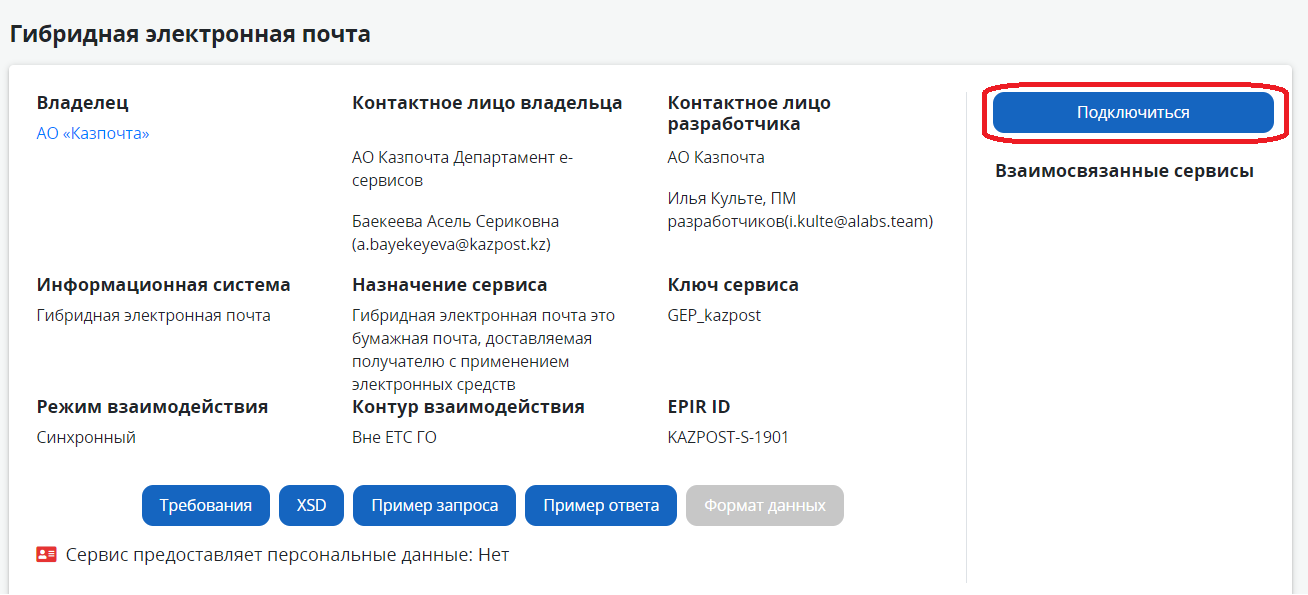
После того, как найден нужный паспорт сервиса, необходимо открыть его. В паспорте сервиса отображается общая информация о сервисе интеграции: наименование сервиса, организация-Владелец сервиса, контактные лица от Владельца и разработчика веб-сервиса, информационная система, назначение, ключ сервиса, режим взаимодействия (синхронный или асинхронный), контур взаимодействия (в ЕТС или вне ЕТС ГО), EPIR ID (уникальный идентификатор сервиса в ЕПИР, Единой платформе интернет-ресурсов ГО), а также файлы, необходимые для разработки веб-сервиса подключения – xsd, xml примеров запроса и ответа:



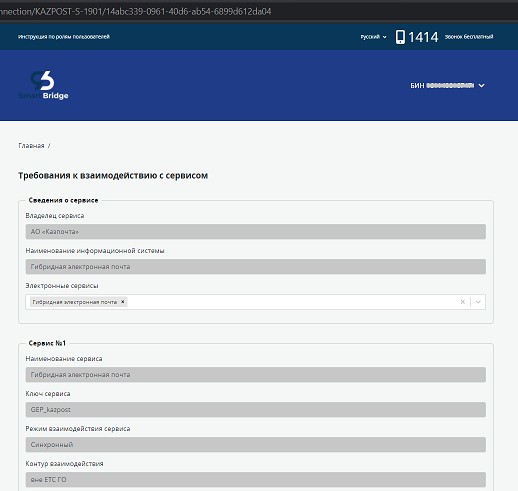
Если пользователь не авторизован на портале, то при попытке скачивания файлов xsd, xml портал Smart Bridge переведет пользователя на страницу авторизации (входа в личный кабинет).

Предполагается, что сначала из паспорта нужного сервиса скачиваются файлы xsd, xml, затем разрабатывается веб-сервис подключения к сервису, далее подается заявка на подключение к сервису.

Для инициирования заявки на подключение к выбранному сервису необходимо в его паспорте нажать на кнопку «Подключиться»:

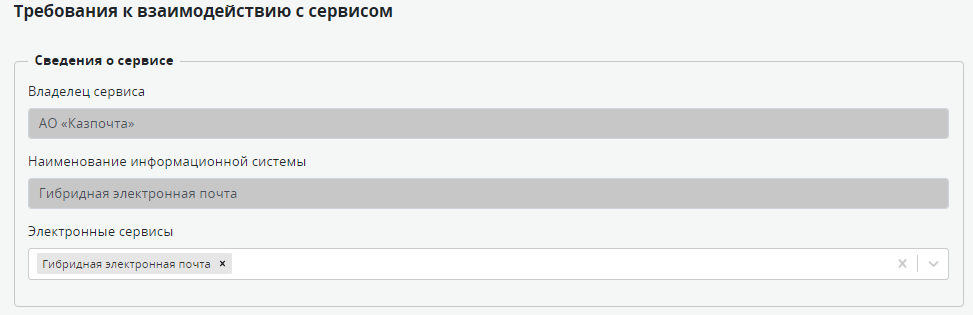


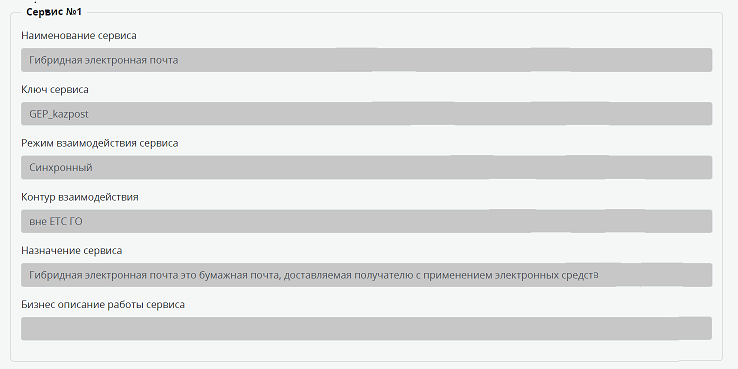
Отобразится страница «Требования к взаимодействию с сервисом»:



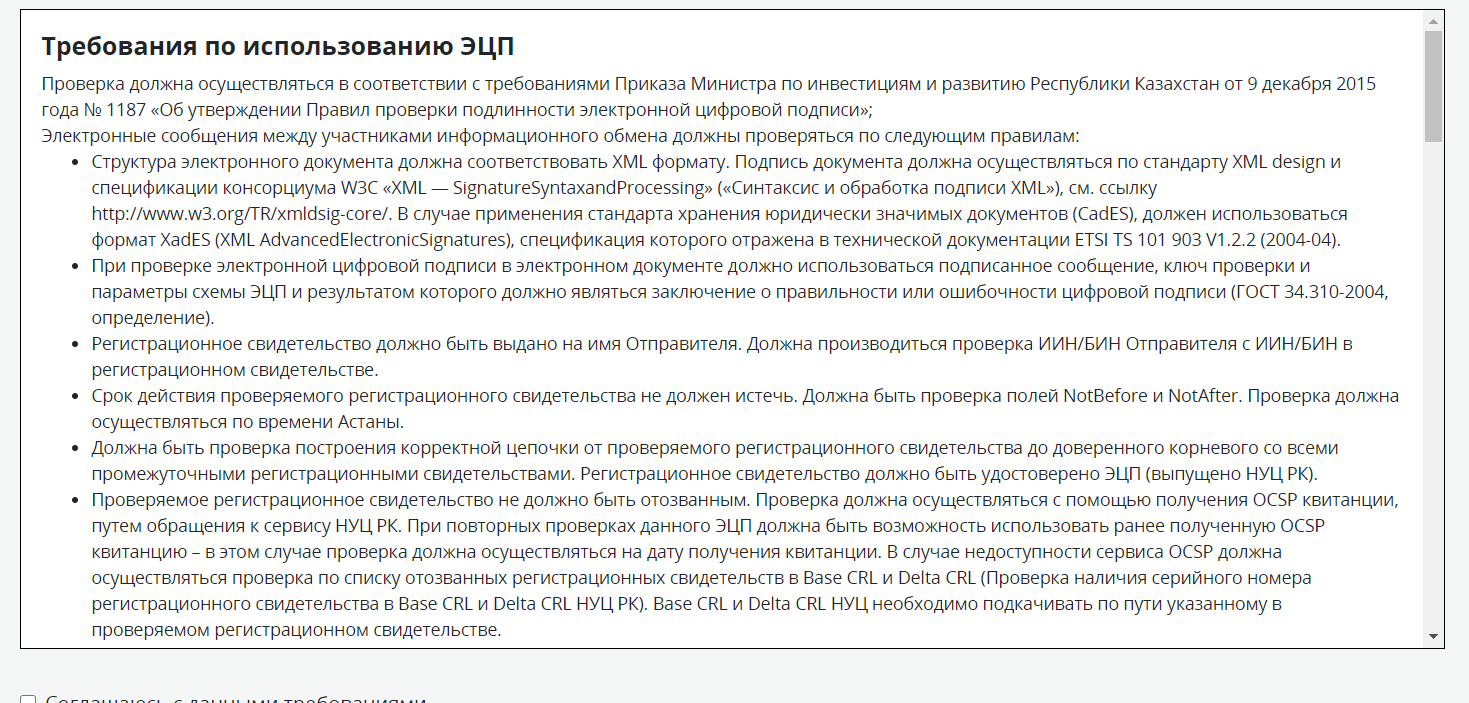
**! Одностороннее выставление Требований со стороны Владельца сервиса, а также подписание на портале Smart Bridge акта тестирования заменяют заключение Соглашения между участниками интеграции.**

Страница «Требования к взаимодействию с сервисом» содержит общую информацию о сервисе из его паспорта, а также требования к интеграции с выбранным сервисом: рекомендуемые требования по производительности и надежности, требования по использованию ЭЦП, требования по информационной безопасности, требования к формату Журнала логирования, требования со стороны ШЭП/ВШЭП:

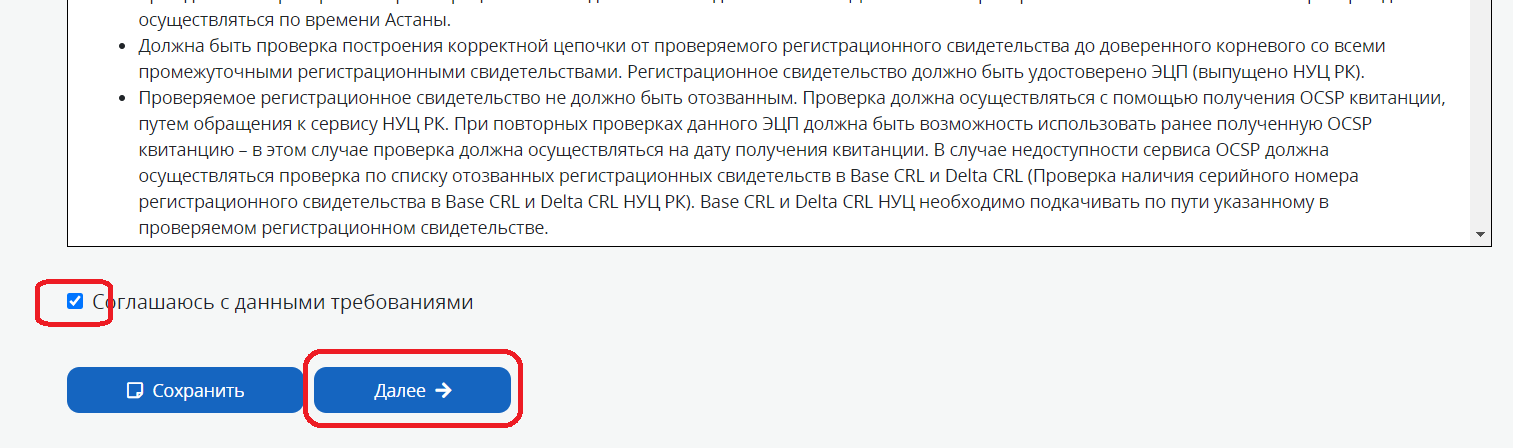




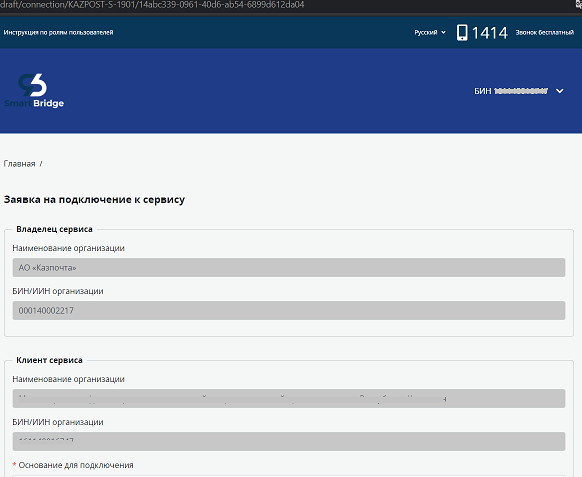




На данной странице не требуется ничего вводить, следует согласиться с данными требованиями и нажать на кнопку «Далее»:

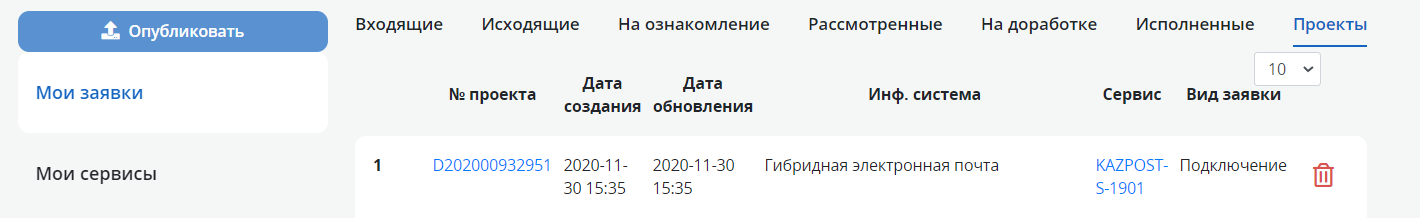


Отобразится страница «Заявка на подключение к сервису» для заполнения заявки:



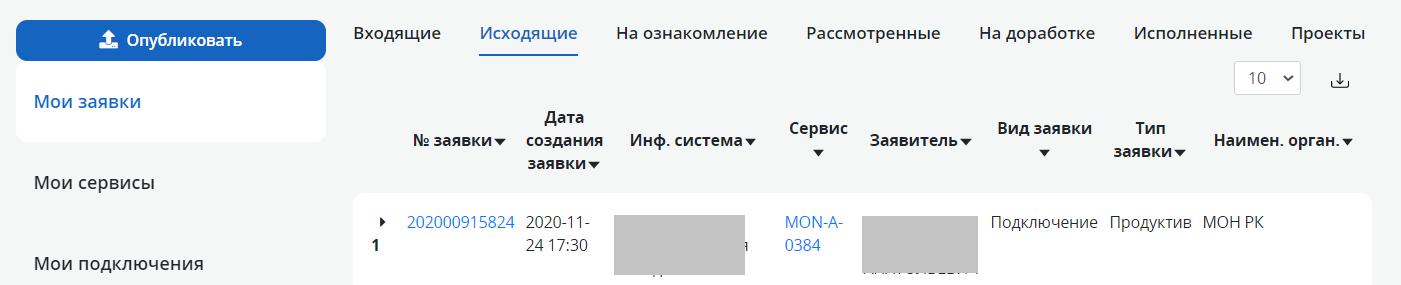
На странице «Заявка на подключение к сервису» поля, выделенные заливкой серого цвета, заполнять не требуется (они получены автоматически из паспорта сервиса, ЭЦП сотрудника, инициировавшего заявку, а также заполнены согласно Правилам интеграции (стандартные требования некоторых полей блока «Данные VPN-туннеля»)). Необходимо заполнить все 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.**

После подписания заявка на подключение к сервису поступает на рассмотрение к Владельцу сервиса.

Владелец сервиса должен рассмотреть заявку в течение двух рабочих дней. При этом, Владелец сервиса имеет возможность отказать или отправить заявку на доработку с указанием причины, а также согласовать реализацию интеграции.

После согласования Владельцем сервиса заявка поступает на рассмотрение в АО «НИТ». В случае корректного заполнения заявка принимается в работу АО «НИТ», проводятся работы по проверке технической возможности интеграции, организации доступа по сети и подключению Клиента к сервису на тестовой среде ШЭП/ВШЭП. 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.

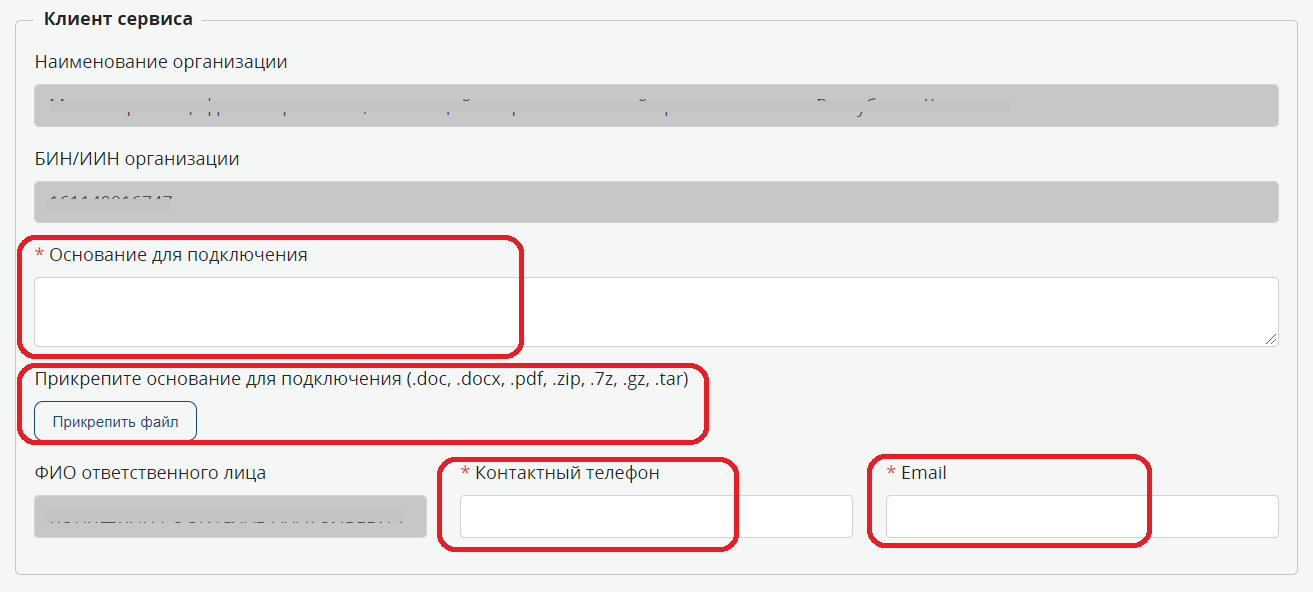
Затем Клиент и Владелец сервиса проводят тестирование, в рамках текущей заявки подписывают акт тестирования (инициирует Клиент сервиса). Далее АО «НИТ» на основании акта тестирования и наличия сообщений на тестовом ШЭП/ВШЭП подключает Клиента к сервису. После жизненный цикл заявки завершается, и она переходит в папку «Исполненные» в личном кабинете инициатора заявки.

Пояснения к заполнению полей

*«Основание для подключения»* – это документ, на основании которого реализуется данная интеграция, т.е. протокол, официальное письмо, дорожная карта, приказ и т.д., например, письмо МЦРИАП РК исх. № 12345 от 05.05.2020 г. касательно интеграции ИС ЕСЭДО и ИС ГС, протокол совещания №1 от 10.10.2020 г.

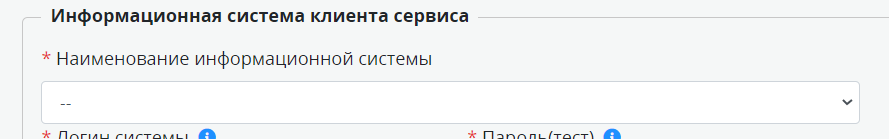
*«Прикрепите основание для подключения (.doc, .docx, .pdf, .zip, .7z, .gz, .tar)»* – необязательное поле, в нем прикрепляется файл основания, например, файл с письмом в формате MS Word. Поддерживается прикрепление файлов с расширениями: .doc, .docx, .pdf, .zip, .7z, .gz, .tar.

*«Контактный телефон», «Email»* – здесь указываются данные лица, которое компетентно ответить на вопросы по данным в подаваемой заявке:



**! В соответствии с политикой Google при отправке архивных файлов с паролем на почтовые адреса gmail.com возможны ошибки доставки письма. Попробуйте указать адрес корпоративной почты или иной почты (например, mail.ru, yandex.ru).**

*«Наименование информационной системы»* – необходимо выбрать из выпадающего списка информационную систему заявителя:



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.

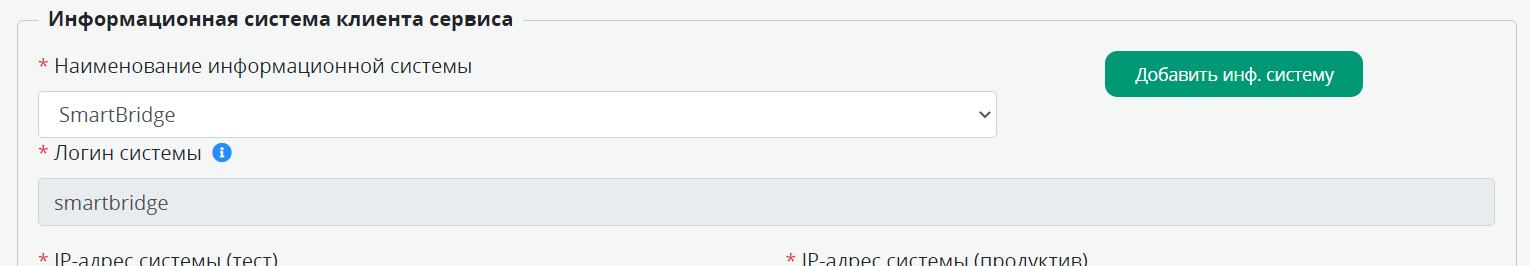
*«Логин системы»* – это логин системы, под которым она будет заведена на ВШЭП, необходимо придумать его и ввести в поле (также сохранить у себя для информации). Логин системы должен быть идентичным в тестовой и промышленной среде ВШЭП. Логин должен содержать как минимум 3 символа, допускается использование 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 ШЭП/ВШЭП либо проводилось ее подключение к веб-сервисам на ШЭП/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/ВШЭП 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.**

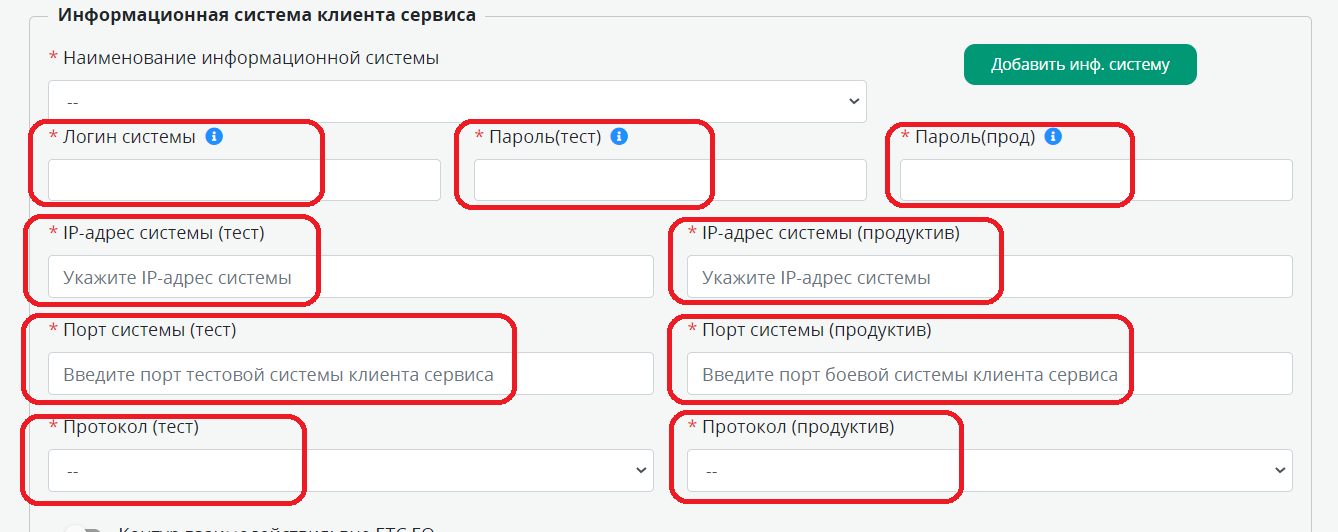
*«Порт системы (тест)»* – это порт, по которому для Клиента будет организовываться доступ к сервису по сети в тестовой среде ВШЭП. Это поле заполняется на усмотрение разработчика веб-сервиса подключения.

«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.



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



«Имеется VPN-туннель для данной системы?» – оставить не активным, если у системы отсутствует VPN-туннель до ВШЭП (ранее не организовывался туннель до ВШЭП):



При наличии действующего VPN-туннеля передвинуть переключатель в активное положение:



Также доступен для скачивания файл с техническими условиями для организации VPN-соединения, данный файл предназначен для специалиста по сетевой инфраструктуре (сетевой администратор, сетевой инженер).

*«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»).

***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.

*«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.