


УТВЕРЖДАЮ
Директор Республиканского
унитарного предприятия
«Национальный центр
электронных услуг»
Р.А.Градусов
« 02 » / « 04 » 2020 г.



ЕДИНЫЕ ТЕХНИЧЕСКИЕ ТРЕБОВАНИЯ
общегосударственной автоматизированной информационной
системы

Минск 2020

СОДЕРЖАНИЕ

1. Термины и определения	3
2. Обозначения и сокращения.....	5
3. Общие положения	7
4. Технические требования к организации взаимодействия Поставщика информации и ОАИС.....	8
5. Технические требования к организации взаимодействия пользователя и ОАИС.....	11
5.1. Требования к Пользователю при получении ЭУ через ЕПЭУ ОАИС ..	11
5.2. Требования к информационному посреднику при подключении к подсистеме «Информационный посредник электронных услуг ОАИС».....	12
5.3. Требования к Пользователю при получении ЭУ по технологии «система-система».....	12
5.3.1. Правила формирования запроса Пользователем	13
5.3.2. Описание кодов состояния HTTP.....	13
5.3.3. Варианты получения ЭУ по технологии «система-система».....	14
6. Технические требования к организации защищенного канала связи.....	16
7. Технические требования к процессу разработки ПО ЭУ (АП).....	18
ПРИЛОЖЕНИЕ А (справочное) Бизнес-процесс оказания услуги по организации защищенного соединения с использованием программного средства канального шифрования «G-SecTLS» (для серверного и клиентского приложений)	20
ПРИЛОЖЕНИЕ Б (справочное) Бизнес-процесс оказания услуги по организации защищенного соединения с использованием программного средства канального шифрования «itVPN».....	21
ПРИЛОЖЕНИЕ В (справочное) Бизнес-процесс разработки ПО ЭУ	22
ПРИЛОЖЕНИЕ Г (справочное) Бизнес-процесс перевода АП в электронную форму.....	23

1. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

В настоящих Единых технических требованиях общегосударственной автоматизированной информационной системы (далее – ЕТТ ОАИС) используются термины и их определения в значениях, установленных Законами Республики Беларусь от 28.10.2008 № 433-З «Об основах административных процедур», от 10.11.2008 № 455-З «Об информации, информатизации и защите информации», от 28.12.2009 № 113-З «Об электронном документе и электронной цифровой подписи», а также следующие термины и определения:

Административный электронный регламент (далее – АЭР) – документ, описывающий организационно-технологический процесс осуществления административной процедуры в электронной форме через единый портал электронных услуг, включая реквизитный состав используемой информации;

Информационный объект – описание субъекта (субъектов) и (или) объекта (объектов) информационных отношений в информационных ресурсах (системах) (далее – ИР (ИС))¹ исходя из назначения ИР (ИС);

ИПЭУ ОАИС – подсистема ОАИС «Информационный посредник электронных услуг ОАИС»;

Интеграция² – организация взаимосвязи ИР (ИС) путем использования единых идентификаторов информационных объектов;

Макет ОАИС - программно-технический комплекс, который предоставляется с целью проведения тестирования программного обеспечения разработанных электронных услуг, административных процедур или информационных ресурсов (систем);

Общегосударственная автоматизированная информационная система – государственная информационная система, предназначенная для обеспечения эффективного электронного информационного взаимодействия в автоматическом и (или) автоматизированном режимах государственных органов, в том числе судов, и государственных организаций между собой, а также с иными организациями, нотариусами и гражданами посредством защищенной информационно-коммуникационной инфраструктуры;

Оператор ОАИС – Республиканское унитарное предприятие «Национальный центр электронных услуг»;

Стенд ОАИС - программно-технический комплекс, который предоставляется с целью разработки программного обеспечения электронных услуг, административных процедур или информационных ресурсов (систем);

¹Для целей ЕТТ ОАИС понятие ИР (ИС), включает в себя также понятие государственный информационный ресурс (система) (далее – ГИР (ГИС)).

² Интегрированные в ОАИС ИР (ИС) могут в дальнейшем использоваться для осуществления АП в электронной форме.

Программный комплекс «Одно окно» — подсистема ОАИС, предназначенная для обеспечения информационного взаимодействия государственных органов и иных организаций и граждан при осуществлении административных процедур, в том числе в электронной форме посредством единого портала электронных услуг;

Поставщик информации – Владелец (и) или Оператор ИР (ИС), подлежащего(их) интеграции с ОАИС;

Пользователь – субъект информационных отношений, получающий информацию, распространяющий и (или) предоставляющий информацию посредством ОАИС, реализующий право на пользование информацией;

Приложение API – группа опубликованных API для обеспечения доступа к электронным услугам, предоставляемым посредством ОАИС, сформированная путем подписки на сервисы Поставщиков информации;

Веб-сервис (сервис) – идентифицируемая веб-адресом программная система со стандартизированными интерфейсами;

Токен доступа – уникальный ключ авторизации для вызова сервиса из числа доступных в рамках конкретного приложения API. Имеет определённый срок действия;

Электронная услуга ОАИС (далее – ЭУ) – услуга, оказываемая Оператором ОАИС на основании соглашения о взаимодействии, заключаемого (заключенного) между Поставщиком информации и Оператором ОАИС, с целью предоставления (получения, изменения, актуализации) информации в электронном виде;

Ядро управления API ОАИС – подсистема взаимодействия с ОАИС, предназначенная для оказания электронных услуг ОАИС (осуществления АП в электронной форме).

2. ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

В настоящих ЕТТ ОАИС используются следующие обозначения и сокращения:

АП	– административная процедура;
АРМ	– автоматизированное рабочее место;
ВЦОД	– виртуальный центр обработки данных;
ГИС	– Государственная информационная система;
ГИР	– Государственный информационный ресурс;
ГосСУОК	– Государственная система управления открытыми ключами проверки электронной цифровой подписи Республики Беларусь;
ЕПЭУ	– единый портал электронных услуг;
ИР	– информационный ресурс;
ИПЭУ	– Информационный посредник электронных услуг ОАИС
ИС	– информационная система;
ОАИС	– общегосударственная автоматизированная информационная система;
ПК	– программный комплекс;
ПО	– программное обеспечение;
РУЦ	– Республиканский удостоверяющий центр;
СКЗИ	– средства криптографической защиты информации;
СМДО	– система межведомственного документооборота государственных органов Республики Беларусь;
ТЗ	– техническое задание;
УИ	– уникальный идентификатор;
ЭЦП	– электронная цифровая подпись;
API	– Application Programming Interface – программный интерфейс приложения;
GUID	– Globally Unique Identifier – статистически уникальный идентификатор;
G-SecTLS	– программный комплект продуктов (серверное и клиентское приложения) для организации защищенного канала передачи данных «G-SecTLS»;
HTTP	– Hyper Text Transfer Protocol – протокол прикладного уровня передачи данных;

HTTPS	– Hyper Text Transfer Protocol Secure – расширение протокола HTTP для поддержки шифрования в целях повышения безопасности;
itVPN	– программный комплекс канального шифрования «itVPN», предназначенный для целей шифрования данных и аутентификации сторон взаимодействия ³ ;
JSON	– JavaScript Object Notation – текстовый формат обмена данными, основанный на JavaScript;
OAuth	– открытый протокол (схема) авторизации, который позволяет предоставить третьей стороне ограниченный доступ к защищённым ресурсам пользователя без необходимости передавать ей (третьей стороне) логин и пароль;
REST	– Representational State Transfer – стиль архитектуры программного обеспечения для распределенных систем, таких как World Wide Web, который, как правило, используется для построения веб-служб;
URL	– Uniform Resource Locator – унифицированный формат адресов электронных ресурсов;
VPN	– Virtual Private Network – виртуальная частная сеть;
WS	– веб-сервис;
WSO2 API Manager (APIM)	– решение для создания, публикации, управления доступом к API и его жизненным циклом.

³ Для целей ЕТТ ОАИС под сторонами взаимодействия подразумеваются ядро API ОАИС и ИР(ИС).

3. ОБЩИЕ ПОЛОЖЕНИЯ

Настоящие ЕТТ ОАИС определяют технические требования к организации взаимодействия:

Поставщика информации и ОАИС;

Пользователя и ОАИС, в том числе при оказании ЭУ и осуществления АП.

ЕТТ ОАИС распространяются на Поставщиков информации и Пользователей и обязательны для исполнения при подключении к ОАИС.

ЕТТ ОАИС описывают отношения: Поставщик информации – ОАИС, Пользователь – ОАИС.

ЕТТ ОАИС разработаны на основании подпункта 5.5 пункта 5 Указа Президента Республики Беларусь от 08.11.2011 № 515 «О некоторых вопросах развития информационного общества в Республике Беларусь», пункта 6 Положения об общегосударственной автоматизированной информационной системе, утвержденного Указом Президента Республики Беларусь от 16.12.2019 № 460.

Все изменения и (или) дополнения к ЕТТ ОАИС утверждаются Оператором ОАИС, размещаются на официальном сайте Оператора ОАИС по адресу в сети Интернет <https://nces.by> (далее – сайт Оператора ОАИС) и вступают в силу с даты их утверждения.

4. ТЕХНИЧЕСКИЕ ТРЕБОВАНИЯ К ОРГАНИЗАЦИИ ВЗАИМОДЕЙСТВИЯ ПОСТАВЩИКА ИНФОРМАЦИИ И ОАИС

Поставщик информации для организации взаимодействия ИР (ИС) с ОАИС обеспечивает:

разработку веб-сервисов, построенных с учетом требований архитектурного стиля REST, в соответствии с требованиями Методики по интеграции информационного ресурса (системы) с ОАИС с использованием ядра управления API ОАИС, утверждённой Оператором ОАИС и размещенной на сайте Оператора ОАИС в разделе «Услуги/Услуги ОАИС/Разработчикам» и на ЕПЭУ (<https://portal.gov.by>) в разделе «Вопросы и ответы/ Разработчикам услуг, владельцам информационных ресурсов» (далее – Методика по интеграции).

Взаимодействие ИР (ИС) с ОАИС осуществляется посредством HTTP-запросов к веб-сервису Поставщика информации. Схема построения взаимодействия Поставщика информации и ОАИС представлена на рисунке 1.

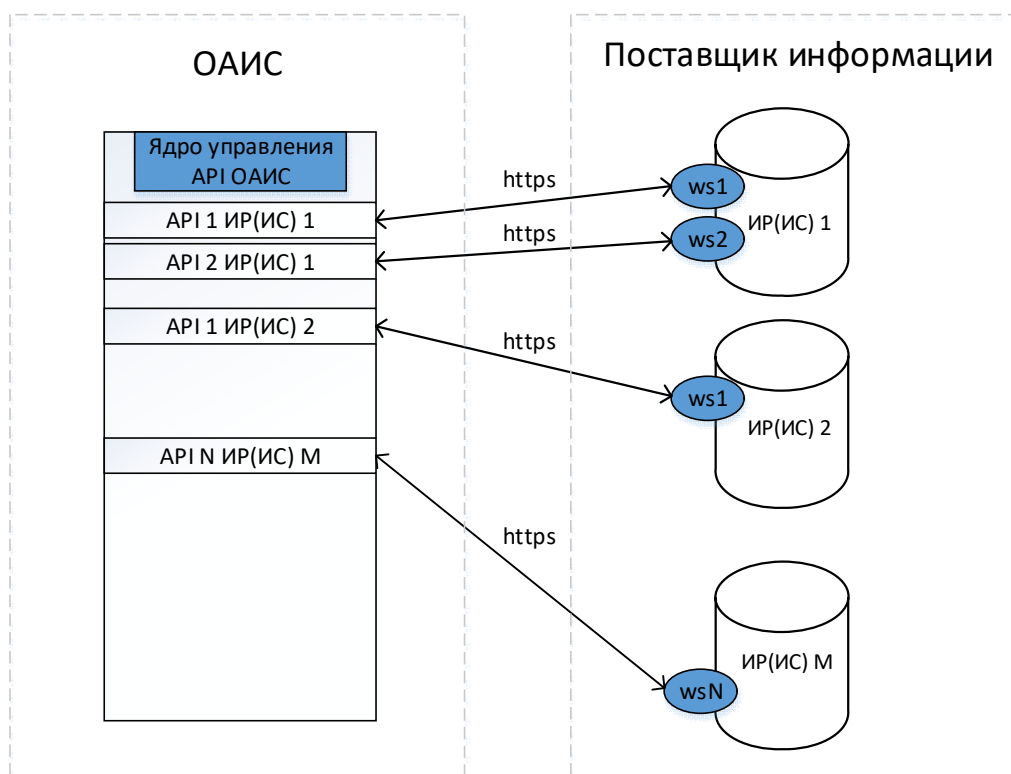


Рисунок 1 – Схема взаимодействия Поставщика информации и ОАИС

Взаимодействие между ИР (ИС) и ОАИС осуществляется по протоколу HTTP(S) с типом передаваемых данных application/json, multipart/form-data, multipart/related.

В целях обеспечения надлежащего оказания ЭУ на основе информации из ИР(ИС) Поставщик информации должен обеспечить выполнение следующих требований.

1. Веб-сервис Поставщика информации, API которого размещается Оператором ОАИС в ядре управления API ОАИС, должен соответствовать следующим параметрам:

коэффициент готовности веб-сервиса, определяющий его отказоустойчивость, должен быть более 99%. Коэффициент готовности веб-сервиса означает вероятность того, что веб-сервис окажется в работоспособном состоянии в произвольный момент времени, кроме планируемых периодов, в течение которых применение объекта по назначению не предусматривается. Расчет осуществляется по формуле $K_{гс} = ((T_{рп} - T_{ро}) / T_{рп}) * 100$, где $T_{рп}$ – период времени, на протяжении которого веб-сервис должен быть в работоспособном состоянии, $T_{ро}$ – период времени простоя (отказа) в течение периода $T_{рп}$;

параметры быстродействия веб-сервиса не должны превышать определенных в таблице 1.

Таблица 1

Объем данных одного запроса к веб-сервису	Количество запросов в единицу времени, при котором не возникает ошибок в работе веб-сервиса	Максимальное время на обработку веб-сервисом запросов: единичного запроса/одного запроса из объема запросов согласно графе 2), в секундах		
		объем данных ответа на один запрос менее 10 Кб	объем данных ответа на один запрос от 10 Кб до 100 Кб	объем данных ответа на один запрос от 100 Кб до 1 Мб
1	2	3	4	5
до 10 Кб	100 запросов/с	0,5/2	1/3	8/10
до 100 Кб	500 запросов/мин	1/3	3/6	10/12
до 1 Мб	50 запросов/мин	8/10	12/30	30/30
до 10 Мб	5 запросов/мин	60/60	60/60	60/60

Параметры быстродействия веб-сервиса при объеме данных одного запроса к веб-сервису более 10 Мб и объеме данных ответа более 1 Мб определяются в каждом конкретном случае экспериментальным путем.

Контроль соответствия веб-сервиса Поставщика информации требуемым параметрам осуществляет Оператор ОАИС во время нагрузочного тестирования веб-сервиса.

2. Поставщик информации должен обеспечить гарантированное резервирование телекоммуникационного маршрута от ИР (ИС) до ОАИС при размещении веб-сервиса на технологической площадке Поставщика информации.

3. Поставщик информации должен предоставить Оператору ОАИС тестовые данные, которые не могут быть интерпретированы как реальные, для организации нагрузочного тестирования веб-сервиса и обеспечения мониторинга работоспособности веб-сервиса.

Подробные требования к Владельцу (Оператору) ИР (ИС), подлежащего интеграции с ОАИС, а также организационные и технические мероприятия по технологическому взаимодействию с ОАИС изложены в Методике по интеграции.

5. ТЕХНИЧЕСКИЕ ТРЕБОВАНИЯ К ОРГАНИЗАЦИИ ВЗАИМОДЕЙСТВИЯ ПОЛЬЗОВАТЕЛЯ И ОАИС

Схема построения взаимодействия Пользователя и ОАИС представлена на рисунке 2.

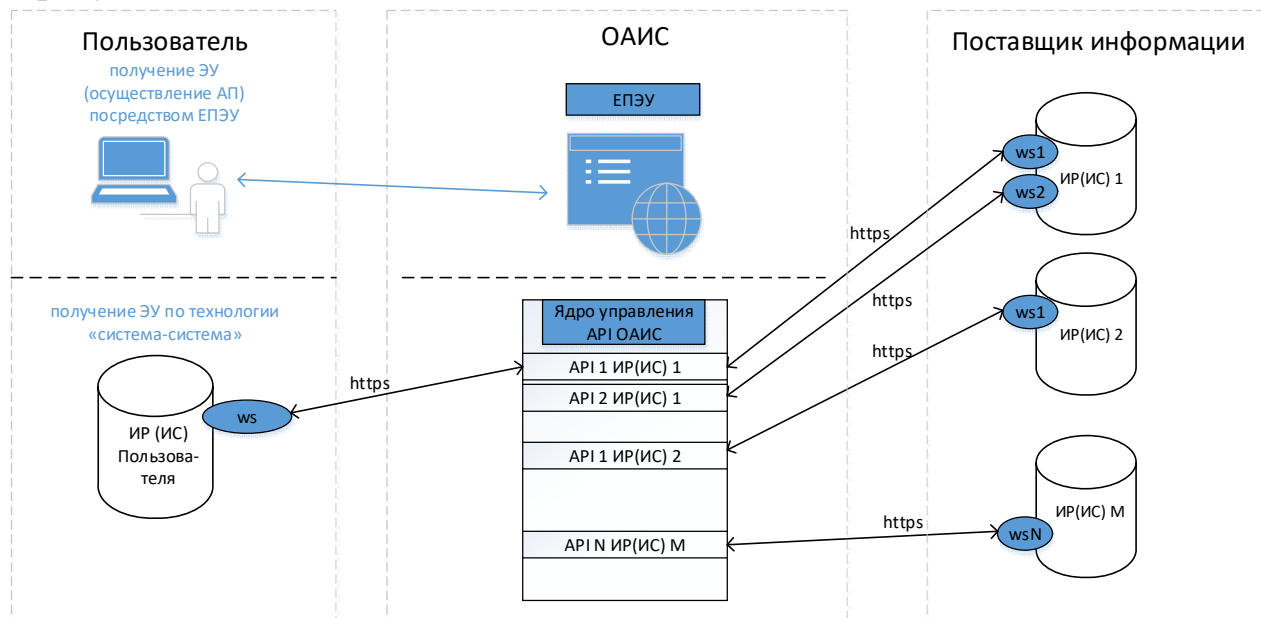


Рисунок 2 - Схема построения взаимодействия Пользователя и ОАИС

5.1. Требования к Пользователю при получении ЭУ через ЕПЭУ ОАИС

Корректная работа Пользователя на ЕПЭУ ОАИС и ПК «Одно окно» обеспечивается при соблюдении требований к рабочему месту Пользователя, указанных в Таблице 2.

Таблица 2

Требования	способ входа на ЕПЭУ ОАИС		подписание электронных документов (независимо от способа входа)	ПК «Одно окно»	ИПЭУ ОАИС (п. 5.2 настоящих ЕТТ ОАИС)
	по электронной почте/ уникальному идентификатору	авторизация с использованием ЭЦП РУЦ ГосСУОК			
ПО					
операционная система Microsoft Windows 7 или выше		0	0	0	0
браузер Microsoft Internet Explorer 9 и выше		0	0	0	0
криптопровайдер «Avest CSP»*		0	0	0	0
персональный менеджер		0	0	0	0

Требования	способ входа на ЕПЭУ ОАИС		подписание электронных документов (независимо от способа входа)	ПК «Одно окно»	ИПЭУ ОАИС (п. 5.2 настоящих ЕТТ ОАИС)
	по электронной почте/ уникальному идентификатору	авторизация с использованием ЭЦП РУЦ ГосСУОК			
сертификатов «Avest PCM»*					
плагин AvCMXWebP*		о	о	о	о
ПО для работы с файлами форматов семейства Microsoft Office, Portable Document Format (PDF)	р	р	р	р	р
антивирусное ПО	р	р	р	о	о
Каналы связи					
Интернет	+	+	+	+	–
VPN-канал со скоростью менее 1 Mb/s	+	+	+	+	+

о – обязательное требование;

р – рекомендация;

+ – возможность подключения;

* – актуальная версия ПО размещается на сайте НЦЭУ по адресу <https://nces.by/pki/>

5.2. Требования к информационному посреднику при подключении к подсистеме «Информационный посредник электронных услуг ОАИС»

Для обеспечения взаимодействия с ИПЭУ ОАИС информационный посредник должен выполнить следующие технические мероприятия:

определить список автоматизированных рабочих мест (далее – АРМ) оператора подсистемы ОАИС «Информационный посредник электронных услуг ОАИС» для организации деятельности по оказанию ЭУ Пользователям;

организовать доступ АРМ к сети передачи данных Оператора ОАИС по VPN-каналу со скоростью не менее 1 Мбит/с. АРМ оператора ИПЭУ ОАИС не должен иметь подключений к сетям электросвязи общего пользования, в том числе к глобальной компьютерной сети Интернет.

5.3. Требования к Пользователю при получении ЭУ по технологии «система-система»

Пользователь должен организовать доступ к сети Оператора ОАИС по VPN-каналу либо по сети Интернет с пропускной способностью, учитывающей количество и частоту запросов к ИР (ИС), а также объем передаваемых данных в рамках информационного обмена с ИР (ИС), но не менее 1 Мбит/с.

В целях получения ЭУ по технологии «система-система» Оператор ОАИС передает Пользователю описание веб-сервиса(ов), содержащее методы веб-сервиса и его параметры к каждой ЭУ.

Доступ к API будет осуществляться по URL в виде: `https://apimgw.core.oais.by:8247/context/version/resource/method`,

где:

`https` – сетевой протокол, используемый для обращения к ядру ОАИС;

`context` – наименование API;

`version` – версия API;

`resource` – наименование ресурса;

`method` – метод веб-сервиса.

Оператор ОАИС обеспечивает доступ Пользователя к журналу обращений к веб-сервисам ИР (ИС). В целях доступа к журналу обращений в заголовке запроса должен передаваться токен доступа.

5.3.1. Правила формирования запроса Пользователем

Передача запроса Пользователя в ИР (ИС) Поставщика информации осуществляется посредством сообщений протокола HTTP с типом содержимого `application/json`.

Структурно HTTP-сообщение состоит из следующих сложений:

заголовков;

параметры метода веб-сервиса;

тела, содержащего запрос/ответ с перечнем атрибутов для определенного веб-сервиса в формате JSON, значения атрибутов.

Заголовок должен содержать:

авторизационный токен доступа (пример: `Authorization: Bearer <access_token>`);

тип содержимого (пример: `Content-Type: application/json`);

иные параметры, определяемые Поставщиком информации.

Получаемый у Оператора ОАИС токен доступа имеет формат GUID (например: `6f9619ff-8b86-d011-b42d-00cf4fc964ff`).

Согласно спецификации протокола OAuth 2.0, полученный токен доступа необходимо передавать в заголовке запроса. При успешной валидации токена доступа в ядре ОАИС, Пользователь проходит авторизацию и имеет право использовать доступный ему перечень веб-сервисов. В случае ошибочной авторизации Пользователю будет отказано в доступе.

Пример передачи токена доступа в заголовке запроса: `curl -k -X GET "https://apimgw.core.oais.by:8247/service/v1/resource/method?parameter=value" -H "accept: application/json" -H "Authorization: Bearer 6f9619ff-8b86-d011-b42d-00cf4fc964ff"`.

5.3.2. Описание кодов состояния HTTP

При работе с ядром ОАИС используются следующие интерпретации кодов состояния HTTP:

401 Unauthorized	Возвращается в случаях несанкционированного доступа к сервису
403 Forbidden	Возвращается в случае, если запрашиваемый ресурс существует, но у клиента недостаточно прав на его просмотр или модификацию
<i>Ошибки соединения</i>	
500 Internal Server Error	
502 Bad Gateway	
504 Gateway Timeout	
<i>Коды состояния, возвращаемые веб-сервисом</i>	
200 OK	Пакет получен
400 Bad Request	Структура пакета неверна
500 Internal Server Error	Непредвиденная ошибка сервера

5.3.3. Варианты получения ЭУ по технологии «система-система»

Получение ЭУ по технологии «система-система» может осуществляться как с использованием очереди сообщений, так и без нее.

Общий алгоритм взаимодействия пользователя с ОАИС:

1. Пользователь формирует HTTP-сообщение в соответствии с правилами, описанными в пункте 5.3.1 ЕТТ ОАИС. Передача параметров метода API производится в соответствии с описанием соответствующего API.

В случае возникновения ошибки при передаче сообщения в ядро ОАИС, Пользователь получает сообщение с кодом состояния об ошибке соединения (с кодом состояния 5XX).

При получении ошибки Пользователь должен направить сообщение повторно. Количество допустимых попыток – 3.

Если количество попыток истекло, а сообщение так и не было передано, Пользователь должен обратиться в службу технической поддержки Оператора ОАИС.

2. Пользователь выполняет запрос в APIМ.

APIМ проверяет токен доступа. В случае возникновения ошибки при авторизации Пользователя, ядро ОАИС возвращает Пользователю сообщение с кодом состояния 401 и описанием ошибки в виде JSON.

APIМ проверяет наличие подписки внешней информационной системы на вызываемый сервис. В случае отсутствия подписки ОАИС возвращает сообщение с кодом состояния 403 и описанием ошибки в виде JSON.

При успешности всех проверок APIМ вызывает метод API. В случае возникновения ошибки при вызове метода API, APIМ возвращает Пользователю сообщение с кодом состояния с кодом состояния 400 и описанием ошибки в виде JSON.

3. Поставщик информации обрабатывает полученный запрос и формирует ответ для Пользователя.

Пользователь получает ответ на запрос в виде JSON.

На этом информационное взаимодействие между Пользователем и Поставщиком информации через ядро ОАИС заканчивается.

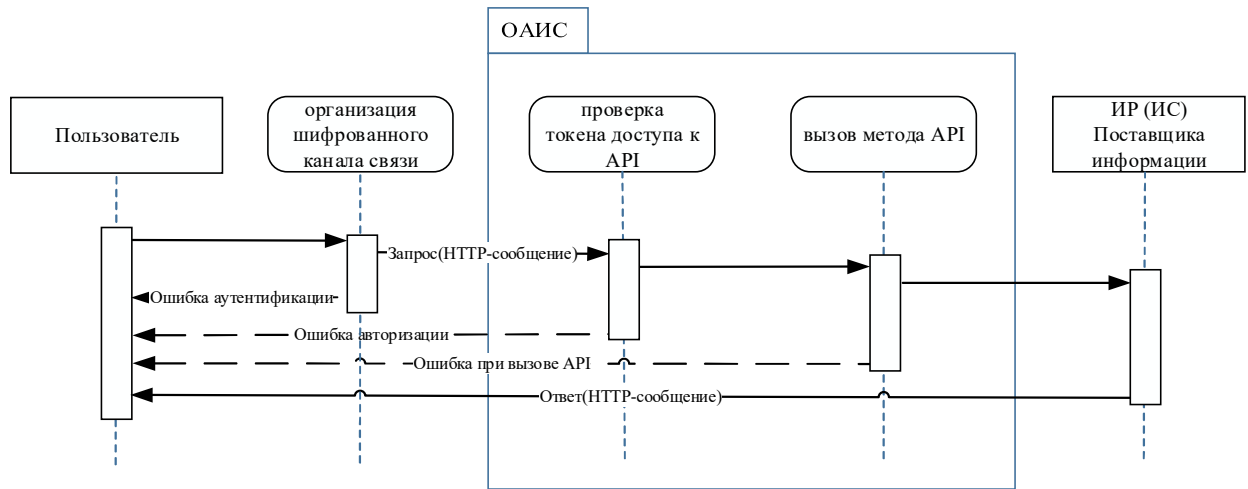


Рисунок 3 – Последовательность обработки запроса в ядре ОАИС

6. ТЕХНИЧЕСКИЕ ТРЕБОВАНИЯ К ОРГАНИЗАЦИИ ЗАЩИЩЕННОГО КАНАЛА СВЯЗИ

Для целей защиты соединения Поставщик информации (Пользователь) использует сертифицированные средства защиты информации, в том числе программный комплект продуктов (серверное и клиентское приложения) для организации защищенного канала передачи данных «G-SecTLS» или программный комплекс канального шифрования «itVPN».

В случае заключения соответствующего договора с Оператором ОАИС посредством организации защищенного канала связи с использованием G-SecTLS Поставщику информации (Пользователю) предоставляются:

- файл закрытого ключа сервиса,
- сгенерированный на основании заявки файл запроса на сертификат открытого ключа,
- сертификат открытого ключа, изданный РУЦ ГосСУОК (сертификат сервиса),
- дистрибутив программного обеспечения «G-SecTLS»,
- документация по установке и настройке.

В случае заключения соответствующего договора с Оператором ОАИС посредством организации защищенного канала связи с использованием itVPN Поставщику информации (Пользователю) предоставляются:

- файл закрытого ключа сервиса,
- сгенерированный на основании заявки файл запроса на сертификат открытого ключа,
- лицензия на itVPN,
- сертификат открытого ключа, изданный РУЦ ГосСУОК (сертификат сервиса),
- документация по установке и настройке itVPN.

Бизнес-процесс оказания услуги по организации защищенного соединения с использованием G-SecTLS приведен в приложении А к ЕТТ ОАИС.

Бизнес-процесс оказания услуги по организации защищенного соединения с использованием itVPN приведен в приложении Б к ЕТТ ОАИС.

Минимальные рекомендуемые требования для серверного и клиентского приложений G-SecTLS:

для архитектуры процессора x86: процессор Intel Celeron и выше / AMD Sempron и выше с тактовой частотой не менее 2 ГГц, объем оперативной памяти 2 ГБ и более, свободное место на жестком диске не менее 80Gb.

Поддерживаемые операционные системы: Windows 7 x 32/64, Windows 8 x 32/64, Windows 8.1 x 32/64, Windows 10 x 32/64, RedHat Linux Enterprise 7 и выше, Suse Linux Enterprise Server 11 и выше, CentOS 7 и выше, Ubuntu 18.04 и выше.

Рекомендуемые характеристики клиентского рабочего места для работы itVPN:

для архитектуры процессора x86: процессор Intel Celeron и выше / AMD Sempron и выше, объем оперативной памяти 1 ГБ и более, свободное место на жестком диске не менее 300МВ;

для архитектуры процессора ARM: процессор ARM Cortex-A7 и выше, объем оперативной памяти 1 ГБ и более, свободное место на жестком диске 300МВ для ОС LINUX/Windows, 30МВ для ОС ANDROID.

Поддерживаемые операционные системы: Android 5 и выше, Oracle Linux v.21 и выше, CentOS 6 и выше, Windows 7 и выше, Windows Server 2008 и выше.

7. ТЕХНИЧЕСКИЕ ТРЕБОВАНИЯ К ПРОЦЕССУ РАЗРАБОТКИ ПО ЭУ (АП) ПО ЭУ (АП)

Для обеспечения процесса разработки ПО ЭУ (АП) должны использоваться следующие программные средства: платформа Oracle 11g, среда разработки JDeveloper, версия 11.1.1.7 (11g Release 1), Eclipse Photon, IntelliJ Idea 2016-2018 Community Edition, NetBeans, Oracle WebCenter.

Выбор иных программных средств, используемых для разработки ПО ЭУ (АП), должен согласовываться с Оператором ОАИС.

Общий алгоритм разработки ПО ЭУ (АП) включает несколько обязательных последовательных этапов:

- разработка веб-сервиса;
- разработка клиента;
- разработка портлета;
- разработка печатной формы.

ЭУ основывается на технологии веб-сервисов и использует взаимодействие с ИР (ИС) для оказания ЭУ.

Бизнес-процесс разработки ПО ЭУ приведен в приложении В к ЕТТ ОАИС.

Бизнес-процесс перевода АП в электронную форму приведен в приложении Г к ЕТТ ОАИС.

При осуществлении АП информационное взаимодействие может быть реализовано:

- с использованием вызовов веб-сервисов ИР (ИС);
- посредством СМДО (модуля АП СМДО);
- посредством ПК «Одно окно».

В случае информационного взаимодействия посредством СМДО и ПК «Одно окно» описание необходимых протоколов взаимодействия со стороны ОАИС передается Оператором ОАИС Поставщику информации для включения в проект соответствующего АЭР.

Описание универсального модуля АП СМДО размещено на сайте Оператора ОАИС по адресу <https://nces.by/wp-content/uploads/Opisanie-modula-AP-SMDO.docx>.

При необходимости реализации функции подписи документов (данных) электронной цифровой подписью в процессе реализации ЭУ (АП) используются средства электронной цифровой подписи, сертификаты открытых ключей которых изданы в РУЦ ГосСУОК.

В целях проверки корректности встраивания в ПО ЭУ (АП) криптографических функций используется демонстрационный сервер закрытого акционерного общества «АВЕСТ» для разработчиков <http://dev.avest.by>.

В случае необходимости использования в ЭУ (АП) справочников могут быть использованы следующие варианты их размещения и обновления:

- размещение в ОАИС с обновлением Поставщиком информации посредством вызова соответствующего API;

размещение на технологической площадке Поставщика информации, обновление Поставщиком информации, обращение к справочнику путем вызова соответствующего API из ЭУ (АП).

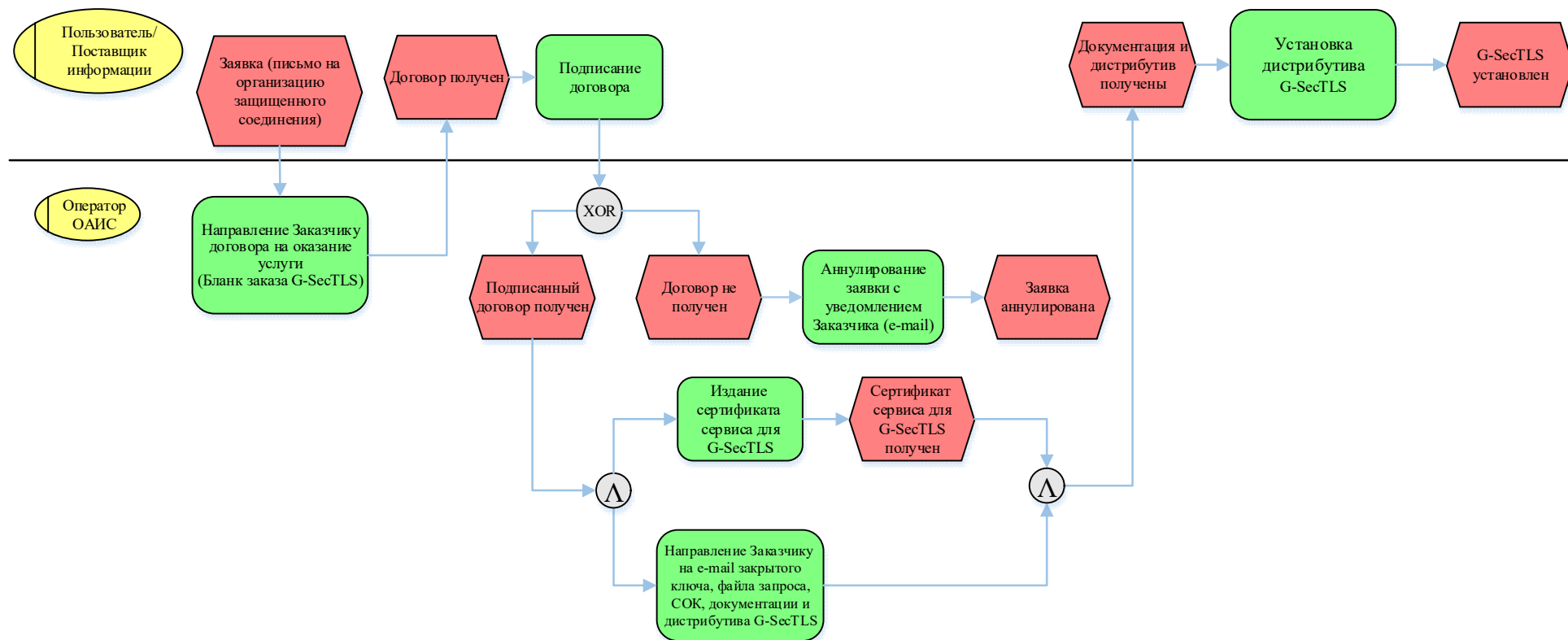
Порядок разработки ПО ЭУ приведён в Методике по интеграции.

Технологический процесс разработки ПО ЭУ описан в Методике разработки электронной услуги ОАИС, утверждённой Оператором ОАИС и размещенной на сайте Оператора ОАИС в разделе «Услуги/Услуги ОАИС/Разработчикам» и на ЕПЭУ (<https://portal.gov.by>) в разделе «Вопросы и ответы/ Разработчикам услуг, владельцам информационных ресурсов».

ПРИЛОЖЕНИЕ А

(справочное)

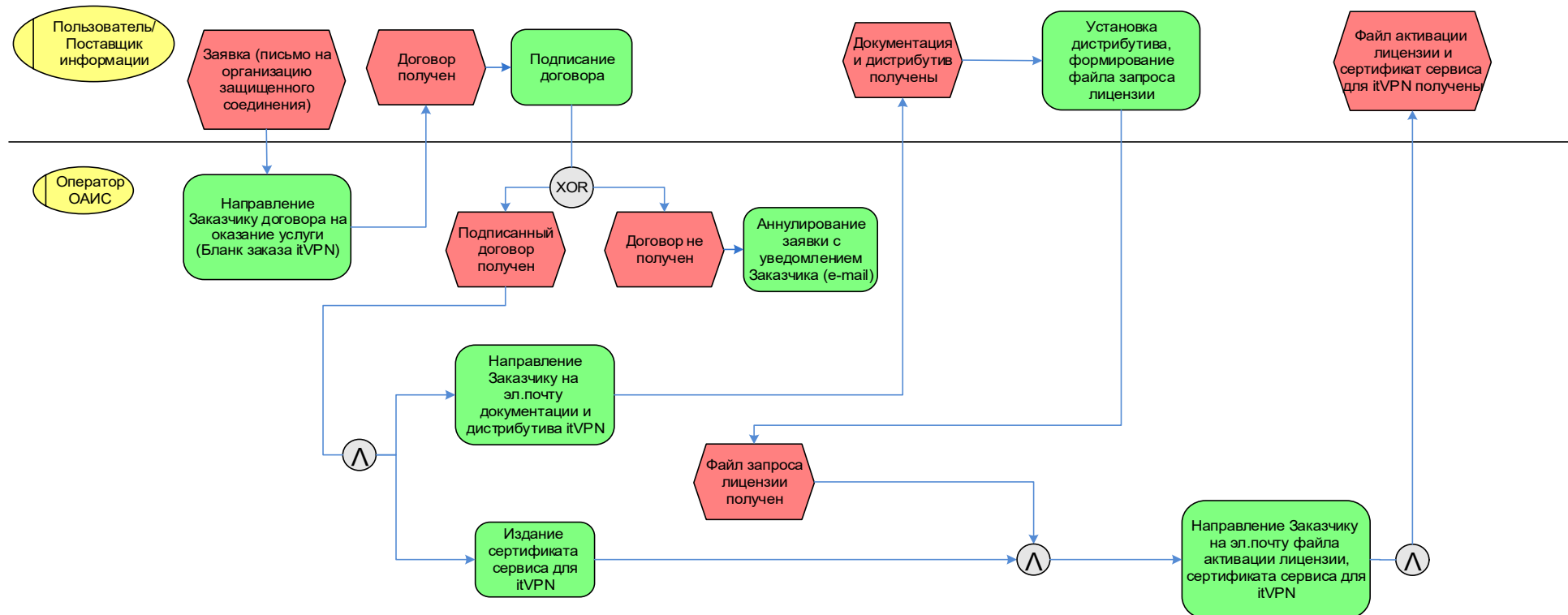
Бизнес-процесс оказания услуги по организации защищенного соединения с использованием программного средства канального шифрования «G-SecTLS» (для серверного и клиентского приложений)



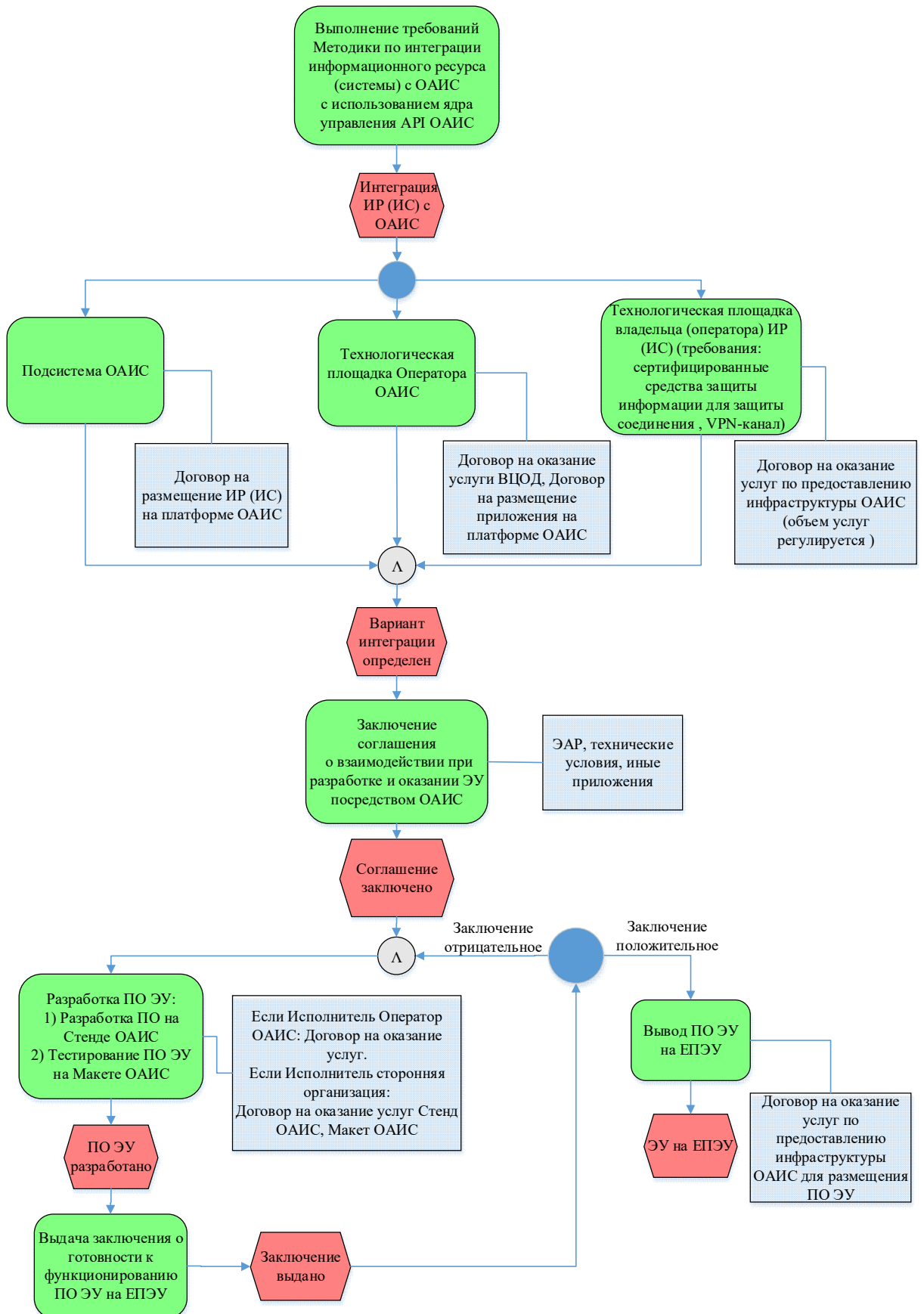
ПРИЛОЖЕНИЕ Б

(справочное)

Бизнес-процесс оказания услуги по организации защищенного соединения с использованием программного средства канального шифрования «ITVPN»



ПРИЛОЖЕНИЕ В
(справочное)
Бизнес-процесс разработки ПО ЭУ



ПРИЛОЖЕНИЕ Г

(справочное)

Бизнес-процесс перевода АП в электронную форму

