ДОПОЛНИТЕЛЬНОЕ СОГЛАШЕНИЕ № 22/2143-Д-10
К ДОГОВОРУ ПРИСОЕДИНЕНИЯ № 22/2143-Д
на оказание услуг, составляющих
лицензируемую деятельность, в отношении шифровальных
(криптографических) средств

г. Москва «01» мая 2018 года

1. Настоящее Дополнительное соглашение в соответствии с пунктом 3.3.1 договора присоединения № 22/2143-Д от 06.07.2012 г. (далее – Договор) вносит изменения (дополнения) в Договор, включая приложения к нему и является неотъемлемой частью Договора.
2. Приложение № 2 к Договору изменяется и излагается в редакции Приложения № 1 к настоящему Дополнительному соглашению.
3. Договор дополняется Приложением № 6, изложенным в редакции Приложения № 2 к настоящему Дополнительному соглашению.
4. Все изменения (дополнения), вносимые настоящим дополнительным соглашением в Договор вступают в силу и становятся обязательными по истечении 30 (тридцати) суток с даты размещения указанных изменений и дополнений в Договоре на сайте Исполнителя по адресу – http:// crypto.rosatom.ru.
5. Во всем остальном, что не установлено настоящим Дополнительным соглашением, действуют условия Договора.

От Исполнителя:
Заместитель директора по информационным технологиям

_____ **С.Н. Данилов**
М.П.
(по доверенности № 22/56/2018-ДОВ
от 26.04.2018)

Приложение № 1 к Дополнительному соглашению №22/2143-Д-10 от 01 мая 2018 г.

к Договору присоединения №22/2143-Д от 06 июля 2012 г.

(Приложение № 2 к Договору присоединения № 22/2143-Д от 06 июля 2012 г.)

Регламент процесса

«Предоставление услуг Корпоративного удостоверяющего центра Госкорпорации «Росатом»

Редакция № 2.4

г. Москва

01.05.2018

Содержание

1. Назначение и область применения

Настоящий регламент Корпоративного Удостоверяющего центра Госкорпорации «Росатом» (далее КУЦ), именуемый в дальнейшем «Регламент», разработан в соответствии с действующим законодательством Российской Федерации, регламентирующим деятельность удостоверяющих центров.

Регламент определяет условия предоставления и правила пользования услугами КУЦ, включая форматы данных, основные организационно-технические мероприятия, направленные на обеспечение работы КУЦ. Регламент имеет статус локального.

Требования настоящего Регламента распространяются на предприятия/ организации использующие автоматизированные и/или информационные системы, в которых применяются сертификаты ключей проверки электронных подписей, создаваемые КУЦ. Требования настоящего Регламента обязательны для выполнения сотрудниками, выполняющими следующие функциональные обязанности:

Руководитель предприятия/организации;

Пользователь КУЦ;

Доверенное лицо;

Оператор КУЦ;

Администратор КУЦ;

Комиссия КУЦ;

Руководитель КУЦ.

Регламент распространяется в форме электронного документа по адресу: URL= http://www.rosatom.ru/ca/docs/regUC/

Регламент использует ссылки на следующие документы, необходимые для администрирования процесса «Предоставление услуг Корпоративного удостоверяющего центра Госкорпорации «Росатом»:

Документ	Статус	Тип документа	Ответственный
Лицензия ФСБ России ЛСЗ №0011890 Рег.№14464 Н от 23.07.2015 на осуществление разработки, производства, распространения шифровальных (криптографических) средств, информационных и телекоммуникационных систем, защищённых с использованием шифровальных (криптографических)	Действует	Лицензия	Данилов С.Н

средств, выполнения работ, оказания услуг в области шифрования информации, технического обслуживания шифровальных (криптографических) средств, информационных и телекоммуникационных систем, защищённых с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных и телекоммуникационных систем, защищённых с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)			
Федеральный закон Российской Федерации от 06.04.2011 № 63-ФЗ «Об электронной подписи»	Действует	Федеральный закон	Данилов С.Н
Приказ ФАПСИ № 152 от 13 июня 2001г. «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну»	Действует	Приказ	Данилов С.Н
Приказ ФСБ РФ от 27 декабря 2011 г. N 795 "Об утверждении Требований к форме квалифицированного сертификата ключа проверки электронной подписи"	Действует	Приказ	Данилов С.Н

Приказ ФСБ РФ от 27 декабря 2011 г. N 796 "Об утверждении Требований к средствам электронной подписи и Требований к средствам удостоверяющего центра"	Действует	Приказ	Данилов С.Н
Приказ Министерства связи и массовых коммуникаций РФ от 23 ноября 2011 г. № 320 “Об аккредитации удостоверяющих центров”	Действует	Приказ	Данилов С.Н
Приказ ГК «Росатом» № 1/1117-П от 23.12.2011 «Об утверждении Положения о системе регламентирующих и методических документов Госкорпорации «Росатом»	Действует	Приказ	Первый заместитель генерального директора ГК «Росатом» Соломон Н.И
Регламент процесса «Организация и обеспечение безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну Госкорпорации «Росатом	Действует	Регламент	Данилов С.Н
Инструкция оператора КУЦ	Действует	Регламент	Данилов С.Н
Порядок подтверждения подлинности электронной подписи в электронном документе	Действует	Регламент	Данилов С.Н

и является основой при регламентации следующих подпроцессов и процедур:

Подпроцессы:	
1.	Предоставление информации в КУЦ

	Процедуры	Предоставление информации доверенным лицом Предоставление информации почтовым сообщением Предоставление информации при личной явке Предоставление информации по e-mail Предоставление информации по телефону Предоставление OCSP запроса Предоставление TSP запроса Предоставление официальной информации для принятия решения КУЦ
2.	Создание сертификата	
3.	Аннулирование сертификата	
4.	Приостановление действия сертификата	
5.	Возобновление действия сертификата	
6.	Подтверждение получения сертификата	
7.	Подтверждение подлинности ЭП в ЭД	
8.	Предоставление сервиса OCSP	
9.	Предоставление сервиса TSP	
10.	Получение информации из КУЦ	
	Процедуры	Получение информации при личной явке Получение информации почтовым сообщением Получение информации доверенным лицом Получение информации через службу Спецсвязи России Получение информации из списков отозванных сертификатов Получение ответа OCSP сервиса Получение ответа TSP сервиса. Получение информации из реестра КУЦ

2. Термины, определения и сокращения

Термин	Определение
Аккредитация	признание уполномоченным федеральным

удостоверяющего центра	органом соответствия удостоверяющего центра требованиям Федерального закона от 6 апреля 2011 г. N 63-ФЗ "Об электронной подписи"
Вручение сертификата ключа проверки электронной подписи	передача доверенным лицом удостоверяющего центра изготовленного этим удостоверяющим центром сертификата ключа проверки электронной подписи его владельцу
Квалифицированный сертификат ключа проверки электронной подписи	сертификат ключа проверки электронной подписи, соответствующий требованиям, установленным настоящим Федеральным законом и иными принимаемыми в соответствии с ним нормативными правовыми актами, и созданный аккредитованным удостоверяющим центром либо федеральным органом исполнительной власти, уполномоченным в сфере использования электронной подписи;
Ключ проверки электронной подписи	уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи (далее - проверка электронной подписи)
Ключ электронной подписи	уникальная последовательность символов, предназначенная для создания электронной подписи
Подтверждение владения ключом электронной подписи	получение удостоверяющим центром, уполномоченным федеральным органом доказательств того, что лицо, обратившееся за получением сертификата ключа проверки электронной подписи, владеет ключом электронной подписи, который соответствует ключу проверки электронной подписи, указанному таким лицом для получения сертификата
Сертификат ключа проверки электронной подписи	электронный документ или документ на бумажном носителе, выданные удостоверяющим центром либо доверенным лицом удостоверяющего центра и подтверждающие принадлежность ключа проверки электронной подписи владельцу

	сертификата ключа проверки электронной подписи
Средства удостоверяющего центра	программные и (или) аппаратные средства, используемые для реализации функций удостоверяющего центра
Средства электронной подписи	шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций - создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи и ключа проверки электронной подписи
Удостоверяющий центр	юридическое лицо, индивидуальный предприниматель либо государственный орган или орган местного самоуправления, осуществляющие функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные настоящим Федеральным законом;
Участники электронного взаимодействия	осуществляющие обмен информацией в электронной форме государственные органы, органы местного самоуправления, организации, а также граждане
Электронная подпись	информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию

Сокращение	Расшифровка
КУЦ	Корпоративный Удостоверяющий центр
Сертификат	Квалифицированный сертификат ключа проверки электронной подписи

COC	Список отозванных сертификатов
ЭД	Электронный документ
ЭП	Электронная подпись
OCSP	Online Certificate Status Protocol
TSP	Time Stamp Protocol

3. Описание процесса

3.1 Цель процесса

Предоставление услуг КУЦ в соответствии с действующим законодательством Российской Федерации.

3.2 Задачи процесса

Данный процесс решает следующие задачи:

- создания сертификатов и выдачи таких сертификатов лицам, обратившимся за их получением (заявителей);
- установления сроков действия сертификатов;
- аннулирования сертификатов, выданных КУЦ;
- приостановления и возобновления действия сертификатов, выданных КУЦ;
- выдачи по обращению заявителя средств ЭП, содержащих ключи ЭП и ключи проверки ЭП, созданные КУЦ;
- ведения реестра выданных и аннулированных сертификатов (далее - реестр сертификатов), в том числе включающего в себя информацию, содержащуюся в сертификатах, и информацию о датах прекращения действия или аннулирования сертификатов и об основаниях таких прекращения или аннулирования;
- создания по обращениям заявителей ключей ЭП и ключей проверки ЭП;
- проверки уникальности ключей проверки ЭП в реестре сертификатов;
- осуществления по обращениям участников электронного взаимодействия проверки ЭП;
- информирования в письменной форме заявителей об условиях и о порядке использования ЭП и средств ЭП, о рисках, связанных с

использованием ЭП, и о мерах, необходимых для обеспечения безопасности ЭП и их проверки;

- обеспечения актуальности информации, содержащейся в реестре сертификатов, и ее защиты от неправомерного доступа, уничтожения, модификации, блокирования, иных неправомерных действий;
- предоставления безвозмездно любому лицу по его обращению в соответствии с установленным порядком доступа к реестру сертификатов информации, содержащейся в реестре сертификатов, в том числе информации об аннулировании сертификатов ключей проверки ЭП;
- обеспечения конфиденциальности созданных КУЦ ключей ЭП;
- осуществления иной, связанной с использованием ЭП деятельности.

3.4 Основные входы процесса

№ п/п	Наименование основного входа процесса	Поставщик основного входа	
		Группа процессов/ внешний контрагент	Уровень управления
1.	Заявление на создание сертификата	Руководитель предприятия	Корпорация
2.	Заявление на аннулирование сертификата	Руководитель предприятия	Корпорация
3.	Заявление на приостановление действия сертификата	Пользователь КУЦ	Корпорация
4.	Заявление на возобновление действия сертификата	Пользователь КУЦ	Корпорация
5.	Заявление на подтверждение подлинности электронной подписи в электронном документе	Руководитель предприятия	Корпорация
6.	Устное обращение на приостановление действия сертификата	Пользователь КУЦ	Корпорация
7.	Копия сертификата ключа проверки электронной подписи на бумажном носителе	Пользователь КУЦ	Корпорация

8.	Скан-копия сертификата ключа проверки электронной подписи на бумажном носителе	Пользователь КУЦ	Корпорация
9.	OCSP запрос	Пользователь КУЦ	Корпорация
10.	TSP запрос	Пользователь КУЦ	Корпорация
11.	Внешнее официальное обращение в КУЦ в части применения электронной подписи	ВСЕ	Корпорация

3.3 Основные выходы процесса

№ п/п	Наименование основного выхода процесса (результата)	Потребитель основного выхода (клиент)	
		Группа процессов/ внешний контрагент	Уровень управления
1.	Ключевой носитель с ключом электронной подписи и сертификатом, Конверт с пин-кодом и парольной фразой и руководством по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи.	Пользователь КУЦ	Организация
2.	Копия сертификата ключа проверки электронной подписи на бумажном носителе	Пользователь КУЦ Оператор КУЦ	Организация
3.	Список отозванных сертификатов (СОС)	Всем	Организация
4.	Заключение о подтверждении подлинности	Заявителю	Организация
5.	OCSP ответ	Заявителю	Организация
6.	TSP ответ	Заявителю	Организация

3.5 Описание подпроцессов

3.5.1 Подпроцесс «Предоставление информации в КУЦ»

Данный подпроцесс регламентирует порядок предоставления информации в КУЦ для создания сертификата, аннулирования сертификата, приостановления действия сертификата, возобновления действия сертификата, подтверждения получения сертификата, подтверждения подлинности ЭП в ЭД, получения сервиса OCSP или получения сервиса TSP.

Пользователь КУЦ предоставляет информацию в КУЦ в виде:

- заявлений в бумажном виде и документов, подтверждающих подлинность данных, внесенных в заявления;
- устных заявлений по телефону;
- обращений по e-mail;
- обращений по протоколу OCSP;
- обращений по протоколу TSP;
- обращений по протоколам HTTP/HTTPS/LDAP.

Пользователь КУЦ предоставляет информацию в КУЦ посредством выполнения процедур:

- предоставления информации по e-mail;
- предоставления информации доверенным лицом;
- предоставления информации почтовым сообщением;
- предоставления информации при личной явке;
- предоставления информации по телефону;
- предоставления OCSP запроса;
- предоставления TSP запроса;
- предоставления официальной информации для принятия решения КУЦ.

3.5.1.1 Процедура «Предоставление информации доверенным лицом»

Для создания сертификата Пользователь КУЦ подготавливает и передаёт доверенному лицу комплект документов, подтверждающих достоверность информации, предоставленной для включения в сертификат, либо их надлежащим образом заверенные копии:

- Заявление на создание квалифицированного сертификата ключа проверки электронной подписи (Приложение №4), заполненное в соответствии с Правилами заполнения заявлений на создание

сертификатов ключей проверки электронной подписи (Приложение №5);

- документ, подтверждающий полномочия Пользователя КУЦ в системе либо доверенность полномочного представителя юридического лица, наделённого правом использования ЭП (Приложение №6);
- доверенность доверенного лица, наделённого правом получения ключевого носителя и сертификата ключа проверки электронной подписи (Приложение №7);
- основной документ, удостоверяющий личность;
- страховое свидетельство государственного пенсионного страхования заявителя (в случае необходимости включения в сертификат поля СНИЛС).

Доверенное лицо прибывает в КУЦ и предъявляет Оператору КУЦ комплект документов.

Оператор КУЦ идентифицирует Доверенное лицо путем проверки документа, удостоверяющего личность и проверяет правильность и полноту поданных документов. Оператор КУЦ переходит к подпроцессу создания сертификата, либо, в случае, если документы заполнены неверно, сообщает об этом Руководителю КУЦ, который принимает решение об отказе в принятии документов.

3.5.1.2 Процедура «Предоставление информации почтовым сообщением»

Пользователь КУЦ подготавливает и отправляет в адрес КУЦ информацию для:

- создания сертификата;
- аннулирования сертификата;
- приостановления действия сертификата;
- возобновления действия сертификата;
- подтверждения подлинности ЭП в ЭД;
- подтверждения факта получения сертификата.

Почтовый адрес КУЦ: 115230, Москва, 1-й Нагатинский проезд., д. 10, стр. 1

Для создания сертификата Пользователь КУЦ подготавливает и отправляет в адрес КУЦ комплект документов, подтверждающих достоверность информации, предоставленной для включения в сертификат, либо их надлежащим образом заверенные копии:

- заявление на создание квалифицированного сертификата ключа проверки электронной подписи (Приложение №4), заполненное в

соответствии с Правилами заполнения заявлений на создание сертификатов ключей проверки электронной подписи (Приложение №5);

- документ, подтверждающий полномочия пользователя КУЦ в системе либо доверенность полномочного представителя юридического лица, наделённого правом использования электронной подписи (Приложение №6);
- основной документ, удостоверяющий личность;
- страховое свидетельство государственного пенсионного страхования заявителя (в случае необходимости включения в сертификат поля СНИЛС).

Для аннулирования сертификата Пользователь КУЦ подготавливает и отправляет в адрес КУЦ Заявление на аннулирование сертификата ключа проверки электронной подписи (Приложение №8).

Для приостановления действия сертификата Пользователь КУЦ подготавливает и отправляет в адрес КУЦ Заявление на приостановление действия сертификата ключа проверки электронной подписи (Приложение №9).

Для возобновления действия сертификата Пользователь КУЦ подготавливает и отправляет в адрес КУЦ Заявление на возобновление действия сертификата ключа проверки электронной подписи (Приложение №10).

Для подтверждения подлинности ЭП в ЭД Пользователь КУЦ подготавливает и отправляет в адрес КУЦ Заявление на подтверждение подлинности электронной подписи в электронном документе (Приложение №11).

Для подтверждения факта получения сертификата Пользователь КУЦ отправляет подписанную копию сертификата ключа проверки электронной подписи (Приложение №12).

После получения документов по почте Оператор КУЦ проверяет правильность и полноту поданных документов и переходит к предоставлению услуги, либо, в случае если документы заполнены неверно, сообщает об этом Руководителю КУЦ, который принимает решение об отказе в принятии документов, а также пользователю УЦ.

В случае поступления в КУЦ почтового сообщения, содержащего иную информацию, обработка данных почтовых сообщений производится Руководителем КУЦ по правилам обработки входящих почтовых сообщений.

3.5.1.3 Процедура «Предоставление информации при личной явке»

Пользователь КУЦ прибывает в КУЦ для:

- создания сертификата;

- аннулирования сертификата;
- приостановления действия сертификата;
- возобновления действия сертификата;
- подтверждения подлинности ЭП в ЭД.

Оператор КУЦ аутентифицирует Пользователя КУЦ путем проверки документа, удостоверяющего личность.

Для создания сертификата Пользователь КУЦ предоставляет в КУЦ комплект документов, подтверждающих достоверность информации, предоставленной для включения в квалифицированный сертификат, либо их надлежащим образом заверенные копии:

- Заявление на создание квалифицированного сертификата ключа проверки электронной подписи (Приложение №4), заполненное в соответствии с Правилами заполнения заявлений на создание сертификатов ключей проверки электронной подписи (Приложение №5);
- документ, подтверждающий полномочия пользователя КУЦ в системе либо доверенность полномочного представителя юридического лица, наделённого правом использования электронной подписи (Приложение №6);
- основной документ, удостоверяющий личность;
- страховое свидетельство государственного пенсионного страхования заявителя (в случае необходимости включения в сертификат поля СНИЛС).

Для аннулирования сертификата Пользователь КУЦ подготавливает и отправляет в адрес КУЦ «Заявление на аннулирование сертификата ключа проверки электронной подписи» (Приложение №8).

Для приостановления действия сертификата Пользователь КУЦ подготавливает и отправляет в адрес КУЦ «Заявление на приостановление действия сертификата ключа проверки электронной подписи» (Приложение №9).

Для возобновления действия сертификата Пользователь КУЦ подготавливает и отправляет в адрес КУЦ «Заявление на возобновление действия сертификата ключа проверки электронной подписи» (Приложение №10).

Для подтверждения подлинности ЭП в ЭД Пользователь КУЦ подготавливает и отправляет в адрес КУЦ «Заявление на подтверждение подлинности электронной подписи в электронном документе» (Приложение №11).

Оператор КУЦ рассматривает предоставленные документы на правильность и полноту и переходит к предоставлению услуги, либо, в

случае если документы заполнены неверно, сообщает об этом Руководителю КУЦ, который принимает решение об отказе в принятии документов.

3.5.1.4 Процедура «Предоставление информации по e-mail»

Процедура используется для восстановления действия сертификата в случае приостановления его действия при получении сертификата в КУЦ доверенным лицом, либо службой спецсвязи.

При получении комплекта документов из КУЦ Пользователь КУЦ подписывает две копии сертификата на бумажном носителе и отправляет в адрес КУЦ скан-копию подписанного сертификата.

Официальный E-mail КУЦ: ca@rosatom.ru

При поступлении сообщения e-mail в КУЦ, содержащего скан-копию сертификата, Оператор КУЦ осуществляет сверку полученной копии с информацией, содержащейся в реестре КУЦ. В случае совпадения информации скан-копии сертификата с информацией, содержащейся в реестре КУЦ, Оператор КУЦ производит распечатку скан-копии и сохранение её в архиве КУЦ и переходит к подпроцессу возобновления действия сертификата.

В случае несовпадения информации скан-копии сертификата с информацией, содержащейся в реестре КУЦ или неправильного оформления копии, Оператор КУЦ сообщает об этом Руководителю КУЦ и он принимает решение об отказе в принятии документов.

В случае поступления в КУЦ сообщения e-mail, не содержащего скан-копию сертификата или содержащего иную информацию, обработка данных сообщений производится Руководителем КУЦ по правилам обработки сообщений электронной почты.

3.5.1.5 Процедура «Предоставление информации по телефону»

При подозрении на компрометацию ключа электронной подписи Пользователь КУЦ может обратиться в КУЦ по телефону для осуществления приостановления действия сертификата.

Для аутентификации по телефону Пользователь КУЦ должен сообщить Оператору КУЦ следующую информацию:

- серийный номер сертификата и данные владельца сертификата, содержащиеся в сертификате, действие которого необходимо приостановить;
- срок, на который приостанавливается действие сертификата;
- ключевую фразу Пользователя КУЦ, содержащуюся в конверте с ключевым носителем.

Заявление принимается только в случае совпадения ключевой фразы с информацией из реестра зарегистрированных Пользователей КУЦ. Принятие решения о приостановлении действия сертификата должно быть осуществлено в течение рабочего дня поступления данного заявления.

В случае получения правильных данных Оператор КУЦ переходит к подпроцессу «Приостановление действия сертификата».

В случае получения неверных данных или невозможности аутентификации Пользователя КУЦ Оператор КУЦ отказывает Пользователю КУЦ в принятии заявления в устной форме.

Не позднее 30 (тридцати) рабочих дней с момента приостановления действия сертификата Пользователь КУЦ должен предоставить в КУЦ Заявление на возобновление действия сертификата ключа проверки электронной подписи (Приложение №10) в том случае, если компрометация ключа ЭП не подтвердилась, в противном случае сертификат аннулируется.

Если факт компрометации ключа ЭП подтвердился, Пользователь КУЦ должен предоставить в КУЦ Заявление на аннулирование сертификата ключа проверки электронной подписи (Приложение №8)

3.5.1.6 Процедура «Предоставление OCSP запроса»

Пользователь КУЦ осуществляет обращение к службе актуальных статусов сертификатов для получения информации о статусе сертификата по протоколу OCSP (Online Certificate Status Protocol) в соответствии с RFC 2560 «X.509 Internet Public Key Infrastructure. Online Certificate Status Protocol – OCSP».

Электронный адрес обращения к Службе актуальных статусов сертификатов КУЦ:

http://ocsp1.rosatom.ru/ocsp/ocsp.srf

http://ocsp2.rosatom.ru/ocsp/ocsp.srf

http://ocsp1.rosatom.local/ocsp/ocsp.srf

http://ocsp2.rosatom.local/ocsp/ocsp.srf

Указанные электронные адреса могут быть занесены в расширение Authority Information Access (AIA) создаваемых КУЦ сертификатов.

Администратор КУЦ отвечает за предоставление ответов службой OCSP в соответствии с процедурой «Получение ответа OCSP сервиса».

3.5.1.7 Процедура «Предоставление TSP запроса»

Пользователь КУЦ осуществляет обращение к службе штампов времени КУЦ для получения штампов времени посредством реализации протокола получения штампа времени TSP (Time-Stamp Protocol),

реализующего RFC 3161 «Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)».

Электронный адрес обращения к Службе штампов времени КУЦ:

http://tsp1.rosatom.ru/tsp/tsp.srf

http://tsp2.rosatom.ru/tsp/tsp.srf

http://tsp1.rosatom.local/tsp/tsp.srf

http://tsp2.rosatom.local/tsp/tsp.srf

Администратор КУЦ отвечает за предоставление ответов службой TSP в соответствии с процедурой «Получение ответа TSP сервиса».

3.5.1.8 Процедура «Предоставление официальной информации для принятия решения КУЦ»

Руководитель КУЦ при получении информации о том, что сертификат содержит недостоверную информацию, принимает решение о приостановлении или аннулировании созданных им сертификатов.

КУЦ по решению суда, вступившему в законную силу, в частности, если решением суда установлено, что сертификат содержит недостоверную информацию, аннулирует созданные им сертификаты.

КУЦ вправе приостановить действие сертификата Пользователя КУЦ в случаях компрометации или подозрения на компрометацию ключа ЭП Пользователя КУЦ в том случае, если Пользователю КУЦ не было известно о возможном факте компрометации ключей, а также в случаях неисполнения обязательств Пользователя КУЦ по Договору присоединения. После приостановления действия сертификата Оператор КУЦ сообщает Пользователю КУЦ о наступлении события, повлекшего приостановление действие сертификата, и уведомляет его о том, что действие сертификата Пользователя КУЦ приостановлено.

3.5.2 Подпроцесс «Создание сертификата»

Подпроцесс «Создание сертификата» регламентирует создание сертификатов КУЦ.

Входящая информация поступает из подпроцесса «Предоставление информации в КУЦ». Исходящая информация поступает в Подпроцесс «Получение информации из КУЦ».

На основании входящей информации Оператор КУЦ устанавливает личность Пользователя КУЦ, либо полномочия лица, выступающего от имени Пользователя КУЦ, по обращению за получением данного сертификата.

Оператор КУЦ с осуществляет проверку достоверности документов и

сведений, представленных Пользователем КУЦ. Оператор КУЦ запрашивает и получает из государственных информационных ресурсов:

1) выписку из единого государственного реестра юридических лиц в отношении заявителя - юридического лица;

2) выписку из единого государственного реестра индивидуальных предпринимателей в отношении заявителя - индивидуального предпринимателя;

3) выписку из Единого государственного реестра налогоплательщиков в отношении заявителя - иностранной организации.

В случае если полученные сведения подтверждают достоверность предоставленной информации, Оператор КУЦ с помощью АРМ Оператора КУЦ проверяет факт регистрации Пользователя КУЦ в реестре КУЦ. В случае отсутствия данных Пользователя КУЦ в реестре КУЦ Оператор КУЦ производит регистрацию в соответствии с «Инструкцией оператора Корпоративного удостоверяющего центра Госкорпорации «Росатом». В противном случае аккредитованный удостоверяющий центр отказывает заявителю в выдаче квалифицированного сертификата.

Оператор КУЦ сохраняет заявления на создание сертификатов ключей проверки электронных подписей в реестре КУЦ и формирует комплект документов для передачи в подпроцесс «Получение информации из КУЦ».

Оператор КУЦ создает уникальный ключ ЭП и сертификат, соответствующий формату, определённому в Приложении №13, на ключевом носителе в соответствии с выбранными Пользователем Ограничениями использования сертификатов ключей проверки электронной подписи, определёнными в Приложении №15.

Оператор КУЦ распечатывает две копии сертификата на бумажном носителе по форме, определённой в Приложении №12, заверяет их личной подписью и печатью КУЦ.

Оператор КУЦ распечатывает конверт с ключевой фразой и пин-кодом, а также «Руководство по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной ЭП» (Приложение №14).

Оператор КУЦ приостанавливает действие сертификата до подтверждения получения Пользователем КУЦ комплекта документов, за исключением предоставления информации при личной явке Пользователя КУЦ.

Оператор КУЦ направляет в единую систему идентификации и аутентификации сведения о лице, получившем квалифицированный сертификат, в объеме, необходимом для регистрации в единой системе идентификации и аутентификации, и о полученном им квалифицированном сертификате.

Оператор несет личную ответственность за правильность внесения данных из заявления на создание сертификат в реестр КУЦ.

Руководитель КУЦ осуществляет планирование, контроль показателей и управление подпроцессом.

3.5.3 Подпроцесс «Аннулирование сертификата».

Подпроцесс «Аннулирование сертификата» регламентирует аннулирование сертификатов КУЦ.

Входящая информация поступает из подпроцесса «Предоставление информации в КУЦ». Исходящая информация поступает в Подпроцесс «Получение информации из КУЦ».

КУЦ должен официально уведомить Пользователя КУЦ и всех лиц, зарегистрированных в КУЦ, об аннулировании сертификата не позднее одного рабочего дня с момента наступления описанного события.

КУЦ аннулирует сертификат Пользователя КУЦ в следующих случаях:

- по Заявлению на аннулирование сертификата ключа проверки электронной подписи Пользователя КУЦ.
- по заявлению Руководителя предприятия/организации Пользователя КУЦ в случае отзыва доверенности Пользователя КУЦ или изменении его полномочий;
- по истечении срока, на который действие сертификата было приостановлено, аннулирование производится автоматически;
- в случае прекращения действия Договора;
- в случае, если не подтверждено, что владелец сертификата ключа проверки электронной подписи владеет ключом электронной подписи, соответствующим ключу проверки электронной подписи, указанному в таком сертификате;
- в случае, если установлено, что содержащийся в таком сертификате ключ проверки электронной подписи уже содержится в ином ранее созданном сертификате ключа проверки электронной подписи;
- в случае, если вступило в силу решение суда, которым, в частности, установлено, что сертификат ключа проверки электронной подписи содержит недостоверную информацию.
- при компрометации ключа ЭП Уполномоченного лица КУЦ. Временем аннулирования сертификата Пользователя КУЦ признается время компрометации ключа Уполномоченного лица КУЦ, фиксирующееся в реестре КУЦ.

Оператор КУЦ осуществляет обработку заявления на аннулирование сертификата ключа проверки электронной подписи и вносит информацию об аннулировании в реестр КУЦ. Обработка заявления на аннулирование ключа проверки электронной подписи должна быть осуществлена не позднее рабочего дня следующего за рабочим днем, в течение которого указанное заявление было принято КУЦ.

3.5.4 Подпроцесс «Приостановление действия сертификата»

Подпроцесс «Приостановление действия сертификата» регламентирует приостановление действия сертификатов КУЦ.

Входящая информация поступает из подпроцесса «Предоставление информации в КУЦ». Исходящая информация поступает в подпроцесс «Получение информации из КУЦ».

КУЦ приостанавливает действие сертификата Пользователя КУЦ в следующих случаях:

- по заявлению на приостановление действия сертификата ключа проверки электронной подписи Пользователя КУЦ;
- по заявлению Пользователя КУЦ в устной форме по телефону;
- в иных случаях, предусмотренных положениями настоящего Регламента, по решению КУЦ.

Обработка заявления на приостановление действия сертификата ключа проверки электронной подписи в бумажной форме должна быть осуществлена Оператором УЦ не позднее рабочего дня следующего за рабочим днём, в течение которого заявление было принято КУЦ.

Оператор КУЦ приостанавливает действие сертификата ключа проверки ЭП Пользователя КУЦ и заносит об этом информацию в реестр КУЦ.

Действие сертификата приостанавливается на исчисляемый в днях срок. Минимальный срок приостановления действия сертификата составляет 30 (тридцать) дней.

Если в течение срока приостановления действия сертификата действие этого сертификата не будет возобновлено, то данный сертификат аннулируется КУЦ.

3.5.5 Подпроцесс «Возобновление действия сертификата».

Подпроцесс «Возобновление действия сертификата» регламентирует возобновление действия сертификатов КУЦ.

Входящая информация поступает из подпроцесса «Предоставление информации в КУЦ». Исходящая информация поступает в подпроцесс «Получение информации из КУЦ».

Оператор КУЦ возобновляет действие сертификата Пользователя КУЦ и вносит информацию об этом в реестр КУЦ по Заявлению на возобновление действия сертификата ключа проверки электронной подписи Пользователя КУЦ. Заявление на возобновление действия сертификата ключа проверки электронной подписи должно быть подано в КУЦ до истечения срока приостановления соответствующего сертификата.

Возобновление действия сертификата ключа и официальное уведомление о возобновлении действия сертификата должны быть осуществлены не позднее рабочего дня следующих за рабочим днем, в течение которого было подано заявление в КУЦ.

3.5.6 Подпроцесс «Подтверждение получения сертификата»

Данный подпроцесс регламентирует подтверждение получения сертификата при передаче сертификата Пользователю КУЦ доверенным лицом либо службой специальной связи.

После получения сертификата Пользователь КУЦ должен ознакомиться с содержанием сертификата, подписать две копии сертификата на бумажном носителе и отправить их в КУЦ в соответствии с подпроцессом «Предоставление информации в КУЦ».

Оператор КУЦ при получении скан-копии сертификата сверяет данные из скан-копии сертификата с информацией, хранящейся в реестре КУЦ. В случае, если данные в скан-копии верны, Оператор КУЦ распечатывает скан-копию сертификата, сохраняет ее в архиве КУЦ и переходит к подпроцессу «Возобновление действия сертификата».

Оператор КУЦ при получении бумажной копии сертификата, подписанной Пользователем КУЦ, сверяет полученные данные с данными из реестра КУЦ. В случае если данные в бумажной копии сертификата верны, Оператор КУЦ сохраняет её в архиве КУЦ и переходит к подпроцессу «Возобновление действия сертификата».

В случае если данные в полученных документах не совпадают с данными в реестре КУЦ, Оператор КУЦ сообщает об этом Руководителю КУЦ, который принимает решение об отказе в принятии документов.

В случае поступления в КУЦ почтового/электронного сообщения, содержащего иную информацию, обработка данных почтовых/электронных сообщений производится Руководителем КУЦ по правилам обработки входящих сообщений почты.

3.5.7 Подпроцесс «Подтверждение подлинности ЭП в ЭД»

Данный подпроцесс регламентирует порядок подтверждения подлинности электронной подписи в электронном документе.

Входящая информация поступает из подпроцесса «Предоставление информации в КУЦ». Исходящая информация поступает в подпроцесс «Получение информации из КУЦ».

КУЦ обеспечивает подтверждение подлинности ЭП в ЭД если формат ЭД с ЭП соответствует стандарту криптографических сообщений Cryptographic Message Syntax (CMS). Решение о соответствии ЭД с ЭП стандарту CMS принимает КУЦ.

Для подтверждения подлинности ЭП в ЭД Пользователь КУЦ предоставляет в КУЦ Заявление на подтверждение подлинности электронной подписи в электронном документе (Приложении №11).

Заявление должно содержать следующую информацию:

- дата и время подачи заявления;
- идентификационные данные Пользователя КУЦ, подлинность ЭП которого необходимо подтвердить в ЭД;
- время и дата формирования ЭП ЭД;
- время и дата, на момент наступления которых требуется установить подлинность ЭП.

Обязательным приложением к заявлению на подтверждение подлинности ЭП в ЭД является электронный носитель, содержащий:

- сертификат, с использованием которого необходимо осуществить подтверждение подлинности ЭП в электронном документе – в виде файла стандарта CMS;
- электронный документ – в виде одного файла (стандарта CMS), содержащего данные и значение ЭП этих данных, либо двух файлов: один из которых содержит данные, а другой значение ЭП этих данных (файл стандарта CMS).

В качестве электронного носителя могут применяться компакт-диски формата CD или DVD. После проведения процедуры подтверждения подлинности ЭП в ЭД предоставленный Пользователем УЦ электронный носитель не возвращается.

Проведение работ по подтверждению подлинности ЭП в ЭД осуществляет комиссия, сформированная из числа сотрудников КУЦ. Комиссия КУЦ проводит работы по подтверждению подлинности ЭП в ЭД в соответствии с методикой проведения подтверждения подлинности.

Результатом проведения работ по подтверждению подлинности ЭП в электронном документе является заключение КУЦ.

Заключение содержит:

- состав Комиссии КУЦ, осуществлявшей проверку;
- основание для проведения проверки;
- результат проверки ЭП в ЭД;
- данные, представленные Комиссии КУЦ для проведения проверки.
- отчет по выполненной проверке.

Отчет по выполненной проверке содержит:

- время и место проведения проверки;
- содержание и результаты проверки;
- обоснование результатов проверки.

Заключение КУЦ по выполненной проверке составляется в произвольной форме в двух экземплярах, подписывается всеми членами Комиссии КУЦ и заверяется печатью КУЦ. Один экземпляр заключения по выполненной проверке предоставляется заявителю.

Срок проведения работ по подтверждению подлинности ЭП в одном ЭД и предоставлению Пользователю КУЦ заключения по выполненной проверке составляет десять рабочих дней с момента поступления заявления в КУЦ.

3.5.8 Подпроцесс «Предоставление сервиса OCSP».

Данный подпроцесс регламентирует порядок предоставления информации о статусе сертификата по протоколу OCSP.

Входящая информация поступает из подпроцесса «Предоставление информации в КУЦ». Исходящая информация поступает в подпроцесс «Получение информации из КУЦ».

Администратор КУЦ отвечает за предоставление ответов службой OCSP в соответствии с процедурой «Получение ответа OCSP сервиса».

3.5.9 Подпроцесс «Предоставление сервиса TSP».

Данный подпроцесс регламентирует порядок предоставления штампов времени по протоколу TSP.

Входящая информация поступает из подпроцесса «Предоставление информации в КУЦ». Исходящая информация поступает в подпроцесс «Получение информации из КУЦ».

Администратор КУЦ отвечает за предоставление ответов службой TSP в соответствии с процедурой «Получение ответа TSP сервиса»

3.5.10 Подпроцесс «Получение информации из КУЦ»

Данный подпроцесс регламентирует порядок получения информации из КУЦ после создания сертификата, аннулирования сертификата, приостановления действия сертификата, возобновления действия сертификата, подтверждения получения сертификата, подтверждения подлинности ЭП в ЭД, получения сервиса OCSP или получения сервиса TSP.

Пользователь КУЦ получает информацию из КУЦ в виде:

- сертификата в бумажном виде;
- ключа ЭП и сертификата на ключевом носителе;
- конверта с ключевой фразой и пин-кодом;
- Руководства по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи в бумажном виде;
- Заключения Удостоверяющего центра о подтверждении подлинности электронной подписи в электронном документе;
- ответов на обращения к списку отозванных сертификатов по протоколам HTTP/HTTPS/LDAP;
- ответов на обращения по протоколу OCSP;
- ответов на обращения по протоколу TSP.

Пользователь КУЦ получает информацию из КУЦ посредством выполнения процедур:

- получения информации при личной явке;
- получения информации почтовым сообщением;
- получения информации через доверенное лицо;
- получения информации через службу Спецсвязи России;
- получения информации из списков отозванных сертификатов;
- получения ответа на OCSP запрос;
- получения ответа на TSP запрос.

3.5.10.1 Процедура «Получение информации при личной явке»

Процедура «Получение информации при личной явке» определяет порядок получения информации Пользователем УЦ от КУЦ после выполнения процедур «Создание сертификата» и «Подтверждение подлинности ЭП в ЭД».

После выполнения подпроцесса «Подтверждение подлинности ЭП в ЭД» Оператор КУЦ аутентифицирует посетителя и проверяет документ удостоверяющий личность.

Оператор КУЦ выдает Пользователю КУЦ первый экземпляр Заключения Удостоверяющего центра о подтверждении подлинности электронной подписи в электронном документе под роспись в Заявлении о подтверждении подлинности электронной подписи в электронном документе. Второй экземпляр Заключения Удостоверяющего центра о подтверждении подлинности электронной подписи в электронном документе Оператор КУЦ сохраняет в архиве УЦ.

После выполнения подпроцесса «Создание сертификата» Оператор КУЦ аутентифицирует посетителя и проверяет документ удостоверяющий личность.

Оператор КУЦ выдает Пользователю КУЦ комплект документов, который в себя включает:

- два экземпляра сертификата в бумажном виде;
- ключ ЭП и сертификат на ключевом носителе;
- конверт с ключевой фразой и пин-кодом;
- «Руководство по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи» в бумажном виде.

Пользователь КУЦ подписывает один экземпляр сертификата в бумажном виде и передает его Оператору КУЦ.

Оператор КУЦ сохраняет в архиве КУЦ экземпляр сертификата в бумажном виде, подписанный Пользователем КУЦ.

3.5.10.2 Процедура «Получение информации почтовым сообщением»

Процедура «Получение информации почтовым сообщением» определяет порядок получения информации Пользователем УЦ от КУЦ после подпроцесса «Подтверждение подлинности ЭП в ЭД».

Входящая информация поступает из подпроцесса «Подтверждение подлинности ЭП в ЭД».

Оператор КУЦ отправляет почтовым сообщением первый экземпляр Заключения Удостоверяющего центра о подтверждении подлинности электронной подписи в электронном документе Пользователю КУЦ с проставлением отметок в Заявлении о подтверждении подлинности электронной подписи в электронном документе.

Второй экземпляр Заключения Удостоверяющего центра о подтверждении подлинности электронной подписи в электронном документе

и Заявление о подтверждении подлинности электронной подписи в электронном документе Оператор КУЦ сохраняет в архиве КУЦ.

3.5.10.3 Процедура «Получение информации доверенным лицом»

Процедура «Получение информации доверенным лицом» определяет порядок получения информации Пользователем УЦ от КУЦ после окончания подпроцесса «Создание сертификата».

Входящая информация поступает из подпроцесса «Создания сертификата». Выходная информация передаётся в подпроцесс «Подтверждение получения сертификата»

Оператор КУЦ аутентифицирует посетителя и проверяет документ удостоверяющий личность, а также Доверенность доверенного лица, наделённого правом получения ключевого носителя и сертификата ключа проверки электронной подписи.

Оператор КУЦ выдаёт Доверенному лицу комплект документов для Пользователя КУЦ, который в себя включает:

- два экземпляра сертификата в бумажном виде;
- ключ ЭП и сертификат на ключевом носителе;
- запечатанный конверт с ключевой фразой и пин-кодом;
- «Руководство по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи» в бумажном виде;

Доверенное лицо передаёт Пользователю КУЦ комплект документов.

Пользователь КУЦ после получения документов из КУЦ подписывает сертификаты, делает скан-копию сертификата. Подписанную скан-копию сертификата Пользователь КУЦ отправляет по e-mail в КУЦ в соответствии с процедурой «Предоставление информации по e-mail». Один подписанный оригинал сертификата Пользователь КУЦ отправляет по почте в КУЦ в соответствии с процедурой «Предоставление информации по почтовым сообщением».

3.5.10.4 Процедура «Получение информации через службу Спецсвязи России»

Процедура «Получение информации через службу Спецсвязи России» определяет порядок получения информации Пользователем УЦ от КУЦ после окончания подпроцесса «Создание сертификата».

Входящая информация поступает из подпроцесса «Создание сертификата».

Оператор КУЦ оформляет пакет документов для Пользователя КУЦ, который в себя включает:

- сопроводительное письмо;
- два экземпляра сертификата в бумажном виде;
- ключ ЭП и сертификат на ключевом носителе;
- конверт с ключевой фразой и пин-кодом;
- Руководство по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи в бумажном виде;

Оператор КУЦ учитывает пакет документов в «Журнале учета исходящих документов» и передаёт сотруднику службы Спецсвязи России.

Сотрудник службы Спецсвязи России доставляет пакет документов на предприятие/организацию Пользователя КУЦ.

3.5.10.5 Процедура «Получение информации из списков отозванных сертификатов»

Процедура «Получение информации из списков отозванных сертификатов» определяет порядок получения информации от КУЦ после окончания подпроцессов «Приостановления действия сертификата», «Аннулирования сертификата», «Возобновления действия сертификата».

Входящая информация поступает из подпроцессов «Приостановления действия сертификата», «Аннулирования сертификата», «Возобновления действия сертификата».

Пользователь КУЦ получает информацию о статусе сертификата из опубликованных на серверах КУЦ списков отозванных сертификатов (СОС).

Официальным уведомлением о факте аннулирования, приостановления или возобновления действия сертификата является опубликование первого (наиболее раннего) списка отозванных сертификатов, содержащего сведения об отозванном сертификате, и изданного не ранее времени наступления произошедшего случая. Временем аннулирования приостановления или возобновления действия сертификата признается время издания указанного списка отозванных сертификатов, хранящееся в поле thisUpdate списка отозванных сертификатов.

Период публикации СОС составляет 12 (двенадцать) часов.

Информация о размещении списка отозванных сертификатов заносится в изданные КУЦ сертификаты ключей подписей в расширение CRL Distribution Point сертификата ключа проверки электронной подписи.

3.5.10.6 Процедура «Получение ответа OCSP сервиса»

Входящая информация поступает из подпроцесса «Предоставление сервиса OCSP».

Пользователь КУЦ получает информацию о статусе сертификата из ответа на OCSP запрос. OCSP-ответы представляются в форме ЭД, подписанного ЭП с использованием сертификата Службы актуальных статусов сертификатов (Оператора Службы актуальных статусов сертификатов).

OCSP-ответ признается действительным при одновременном выполнении следующих условий:

- подтверждена подлинность ЭП Службы актуальных статусов сертификатов (Оператора Службы актуальных статусов сертификатов) в OCSP-ответе;
- сертификат Службы актуальных статусов сертификатов (Оператора Службы актуальных статусов сертификатов) на момент подтверждения подлинности ЭП OCSP-ответа действителен;
- ключ ЭП Службы актуальных статусов сертификатов (Оператора Службы актуальных статусов сертификатов) на момент формирования OCSP-ответа действителен;
- сертификат Службы актуальных статусов сертификатов (Оператора Службы актуальных статусов сертификатов) содержит в расширении Extended Key Usage область использования – Подпись ответа службы OCSP (1.3.6.1.5.5.7.3.9);

3.5.10.7 Процедура «Получение ответа TSP сервиса»

Входящая информация поступает из подпроцесса «Предоставление сервиса TSP».

Пользователь КУЦ получает информацию о штампе времени сертификата из ответа на TSP запрос.

Служба штампов времени по запросам Пользователей КУЦ формирует и предоставляет Пользователям КУЦ штампы времени. Штамп времени, относящийся к подписанному ЭП ЭД, признается действительным при одновременном выполнении следующих условий:

- подтверждена подлинность ЭП Службы штампов времени (Оператора Службы штампов времени) в штампе времени;
- сертификат Службы штампов времени (Оператора Службы штампов времени) на момент подтверждения подлинности ЭП штампа времени действителен;
- ключ ЭП Службы штампов времени (Оператора Службы штампов времени) на момент формирования штампа времени действителен;

- сертификат Службы штампов времени (Оператора Службы штампов времени) содержит в расширении Extended Key Usage область использования – Установка штампа времени (1.3.6.1.5.5.7.3.8);

3.5.10.8 Процедура «Получение информации из реестра КУЦ.

Входящая информация поступает из подпроцессов «Создание сертификата», «Приостановления действия сертификата», «Аннулирования сертификата», «Возобновления действия сертификата».

Пользователь КУЦ получает информацию о статусе и наличии сертификата из реестра выданных и аннулированных КУЦ сертификатов (далее - реестр сертификатов).

Ответственным за предоставление информации из реестра сертификатов является Администратор КУЦ.

4. Нормативные ссылки

Федеральный закон Российской Федерации от 6 апреля 2011 г. N 63-ФЗ "Об электронной подписи".

Приказ ФСБ РФ от 27 декабря 2011 г. N 795 "Об утверждении Требований к форме квалифицированного сертификата ключа проверки электронной подписи".

Приказ ФСБ РФ от 27 декабря 2011 г. N 796 "Об утверждении Требований к средствам электронной подписи и Требований к средствам удостоверяющего центра".

Приказ Министерства связи и массовых коммуникаций РФ от 23 ноября 2011 г. № 320 “Об аккредитации удостоверяющих центров”.

5. Порядок внесения изменений

КУЦ в одностороннем порядке вносит изменения в «Регламент процесса «Предоставление услуг Корпоративного удостоверяющего центра Госкорпорации «Росатом».

Внесение изменений (дополнений) в Регламент, а также в Приложения к нему, производится посредством утверждения новой редакции Регламента. Новая версия Регламента вступает в силу через 30 (тридцать) дней после публикации на сайте КУЦ.

Все Приложения, изменения и дополнения к настоящему Регламенту являются его составной и неотъемлемой частью.

6. Контроль и ответственность

6.1 Контроль выполнения требований Регламента

Пользователь КУЦ несёт ответственность за:

- полноту и своевременность предоставления документов (в соответствии с Приложениями) в КУЦ;
- обеспечение конфиденциальности ключей ЭП, в частности не допущение использования принадлежащих ему ключей ЭП без его согласия;
- уведомление КУЦ, выдавшего сертификат ключа проверки ЭП, и иных участников электронного взаимодействия о нарушении конфиденциальности ключа ЭП в течение не более чем одного рабочего дня со дня получения информации о таком нарушении;
- не использование ключа ЭП при наличии оснований полагать, что конфиденциальность данного ключа нарушена.

Доверенное лицо несёт ответственность за:

- своевременное предоставление документов в КУЦ и за осуществление действий в рамках доверенности;
- сохранность документов и своевременную передачу пакета документов Пользователю;

Оператор КУЦ несёт ответственность за:

- идентификацию и аутентификацию Пользователя КУЦ (Доверенного лица) – проверку представленных документов;
- формирование комплекта документов, выдаваемых КУЦ;
- выдачу Пользователю (Доверенному лицу) комплекта документов (две копии сертификата на бумажном носителе, ключа и сертификата на ключевом носителе, конверта с парольной фразой и пин-кодом, руководства по обеспечению безопасности ЭП, заключения КУЦ подлинности ЭП в ЭД);
- отправку комплекта документов заказным письмом (заключение КУЦ подлинности ЭП в ЭД), сохранение одного экземпляра в архиве КУЦ;
- передачу комплекта документов (две копии сертификата на бумажном носителе, ключа и сертификата на ключевом носителе, конверта с парольной фразой и пин-кодом, руководства по обеспечению безопасности ЭП) сотруднику службы Спецсвязи России и запись в журнале отправки писем;

- за правильность выполнения подпроцессов в соответствии с инструкцией Оператора;
- за конфиденциальность ключей ЭП.

Администратор КУЦ несёт ответственность за:

- правильность настройки и работоспособности ПАК и сервисов OCSP, TSP, CRL;
- за конфиденциальность ключей ЭП КУЦ;

Администратор КУЦ контролирует действия Оператора КУЦ в рамках своих функциональных обязанностей.

Руководитель предприятия/организации несёт ответственность за достоверность предоставляемых документов в КУЦ.

Руководитель КУЦ несёт ответственность за действия Администратора КУЦ и Оператора КУЦ в рамках своих функциональных обязанностей.

6.2 Ответственность работников за несоблюдение требований Регламента

За несоблюдение Регламента ответственные лица несут административную и дисциплинарную ответственность в соответствии с действующим законодательством.

7. Перечень приложений

Приложение №1 Матрица ответственности.

Приложение №2 Схема процесса «Предоставление услуг Корпоративного удостоверяющего центра Госкорпорации «Росатом».

Приложение №3 Дополнительные выходы и дополнительные входы.

Приложение №4 Заявление на создание квалифицированного сертификата ключа проверки электронной подписи.

Приложение №5 Правила заполнения заявлений на создание сертификатов ключей проверки электронной подписи.

Приложение №6 Форма доверенности пользователя Удостоверяющего центра

Приложение №7 Форма доверенности доверенного лица, наделённого правом получения ключевого носителя и сертификата ключа проверки электронной подписи.

Приложение №8 Заявление на аннулирование сертификата ключа проверки электронной подписи.

Приложение №9 Заявление на приостановление действия сертификата ключа проверки электронной подписи.

Приложение №10 Заявление на возобновление действия сертификата ключа проверки электронной подписи.

Приложение №11 Заявление на подтверждение подлинности электронной подписи в электронном документе.

Приложение №12 Форма копии сертификата ключа проверки электронной подписи на бумажном носителе.

Приложение №13 Формат сертификата ключа проверки электронной подписи.

Приложение №14 Руководство по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи.

Приложение №15 Ограничения использования сертификатов ключа проверки электронной подписи.

Приложение №16 Перечень областей использования сертификатов, зарегистрированных в КУЦ.

От Исполнителя:

Заместитель директора по информационным технологиям

_____ С.Н. Данилов

М.П.

(по доверенности № 22/56/2018-ДОВ
от 26.04.2018)

Приложение №1

Матрица ответственности

Подпроцессы в составе процесса	Участники процесса					
	Руководитель предприятия/ организации	Пользователь КУЦ	Доверенное лицо	Оператор КУЦ	Администратор КУЦ	Руководитель КУЦ
1.Подпроцесс «Предоставление информации в КУЦ»	О	О		Инф	К	К
1.1.Процедура «Предоставление информации по e-mail»		О		Инф	К	К
1.2. Процедура «Предоставление информации доверенным лицом»		О	О	Инф	К	К
1.3. Процедура «Предоставление информации почтовым сообщением»		О		Инф	К	К
1.4. Процедура «Предоставление информации при личной явке»		О		Инф	К	К
1.5. Процедура «Предоставление информации по телефону»		О		Инф		К
1.6. Процедура «Предоставление информации по решению КУЦ»		О		Инф	К	О
1.7. Процедура «Предоставление информации OCSP»					О	К
1.8. Процедура «Предоставление информации TSP»					О	К
2. Подпроцесс «Получение информации из КУЦ»		Инф		О	К	К
2.1. Процедура «Получение информации при личной явке»		Инф		О	К	
2.2. Процедура «Получение информации почтовым сообщением»		Инф		О	К	
2.3. Процедура		Инф	О	О	К	

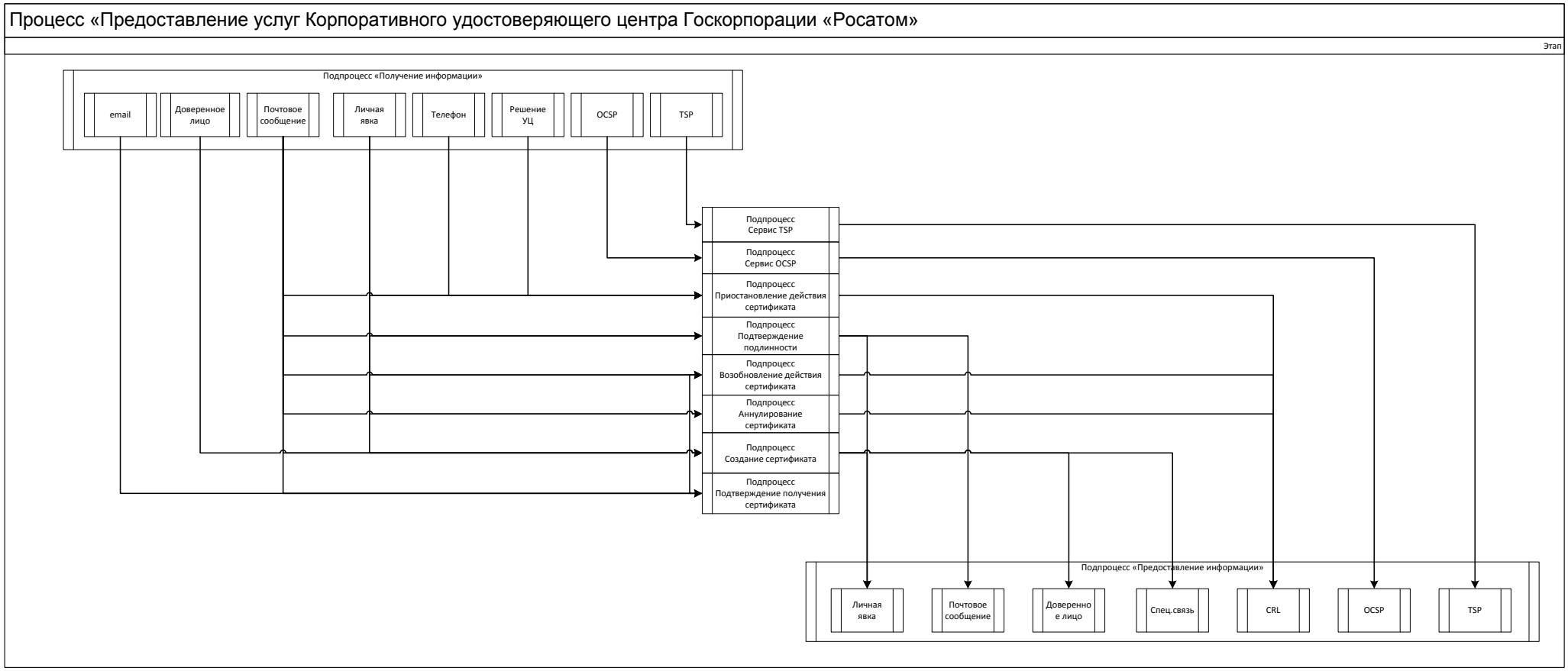
«Получение информации доверенным лицом»						
2.4. Процедура «Получение информации Спецсвязью России»		Инф		О	К	
2.5. Процедура «Получение информации CRL»		Инф			О	К
2.6. Процедура «Получение информации OCSP»		Инф			О	К
2.7. Процедура «Получение информации TSP»		Инф			О	К
3. Подпроцесс «Подтверждение получения сертификата ключа проверки электронной подписи»		О		Инф	К	К
4. Подпроцесс «Создание сертификата ключа проверки электронной подписи»				О	К	К
5. Подпроцесс «Аннулирование сертификата ключа проверки электронной подписи»				О	К	К
6. Подпроцесс «Возобновление действия сертификата ключа проверки электронной подписи»				О	К	К
7. Подпроцесс «Подтверждение подлинности ключа проверки электронной подписи»				О	О	К
8. Подпроцесс «Приостановление действия сертификата ключа проверки электронной подписи»				О	К	К
9. Подпроцесс «Сервис OCSP»					О	К
10. Подпроцесс «Сервис TSP»					О	К

Название (включая сокращение названия) и определение ролей в матрице распределения ответственности и полномочий справочно приведено в таблице ниже:

Сокра-щение	Название роли	Определение	Исполнитель Роли
М	Методолог	Формирует требования к организации деятельности в рамках подпроцесса/процедуры	Структурное подразделение Корпорации/Дивизиона/ Организации
И	Интегратор	Интегрирует результаты подпроцесса/процедуры и отвечает за организацию подпроцесса/процедуры, включая взаимодействие участников	Структурное подразделение Корпорации/Дивизиона/ Организации
К	Контролер	Осуществляет контроль выполнения и достижения результатов подпроцесса/процедуры	Структурное подразделение Корпорации/Дивизиона/ Организации Руководитель Корпорации/Дивизиона/ Организации
О	Ответственный	Несет ответственность за достижение результата по подпроцессу/процедуре в совей предметной области	Структурное подразделение Корпорации/Дивизиона/ Организации Руководитель Корпорации/Дивизиона/ Организации
Утв	Утверждающий	Утверждает - принимает окончательное решение по результату подпроцессу/процедуре	Коллегиальные органы (Наблюдательный совет, Правление и прочие) Генеральный директор Корпорации, Руководители Корпорации /Дивизионов/Организаций
С	Согласовывающий	Согласовывает /одобряет результаты подпроцесса/процедуры для дальнейшего принятия решений	Коллегиальные органы Руководители Корпорации/ Дивизионов/ Организаций
Э	Экспертирующий	Осуществляет экспертизу по подпроцессу/процедуре	Коллегиальные органы Структурное подразделение Корпорации/Дивизиона/ Организации
Инф	Информируемый	Получает информацию о ходе/результате подпроцесса /процедуры	Структурное подразделение Корпорации/Дивизиона/ Организации Руководитель Корпорации/Дивизиона/ Организации Коллегиальные органы

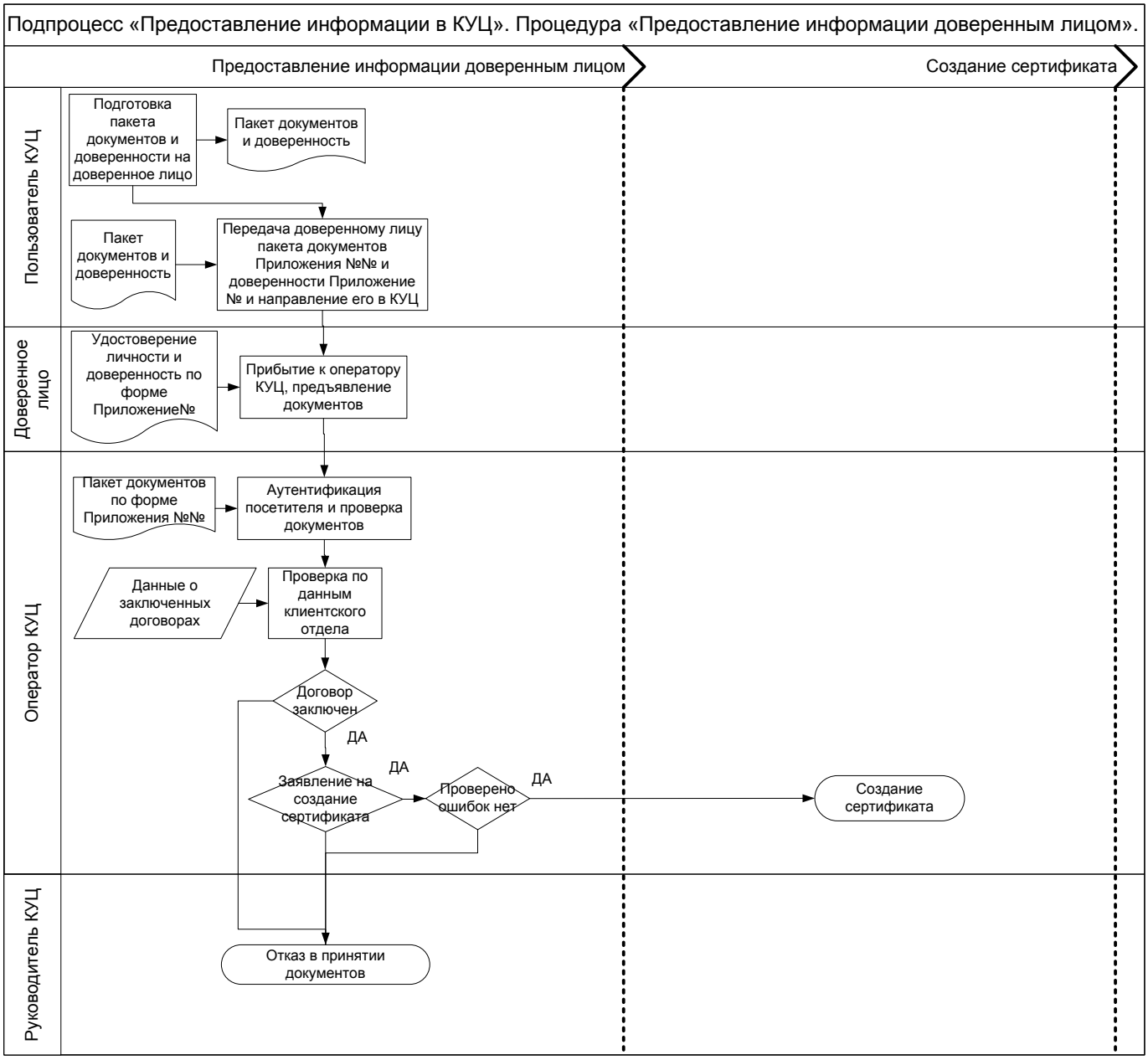
Приложение №2

Схема процесса «Предоставление услуг Корпоративного удостоверяющего центра Госкорпорации «Росатом»

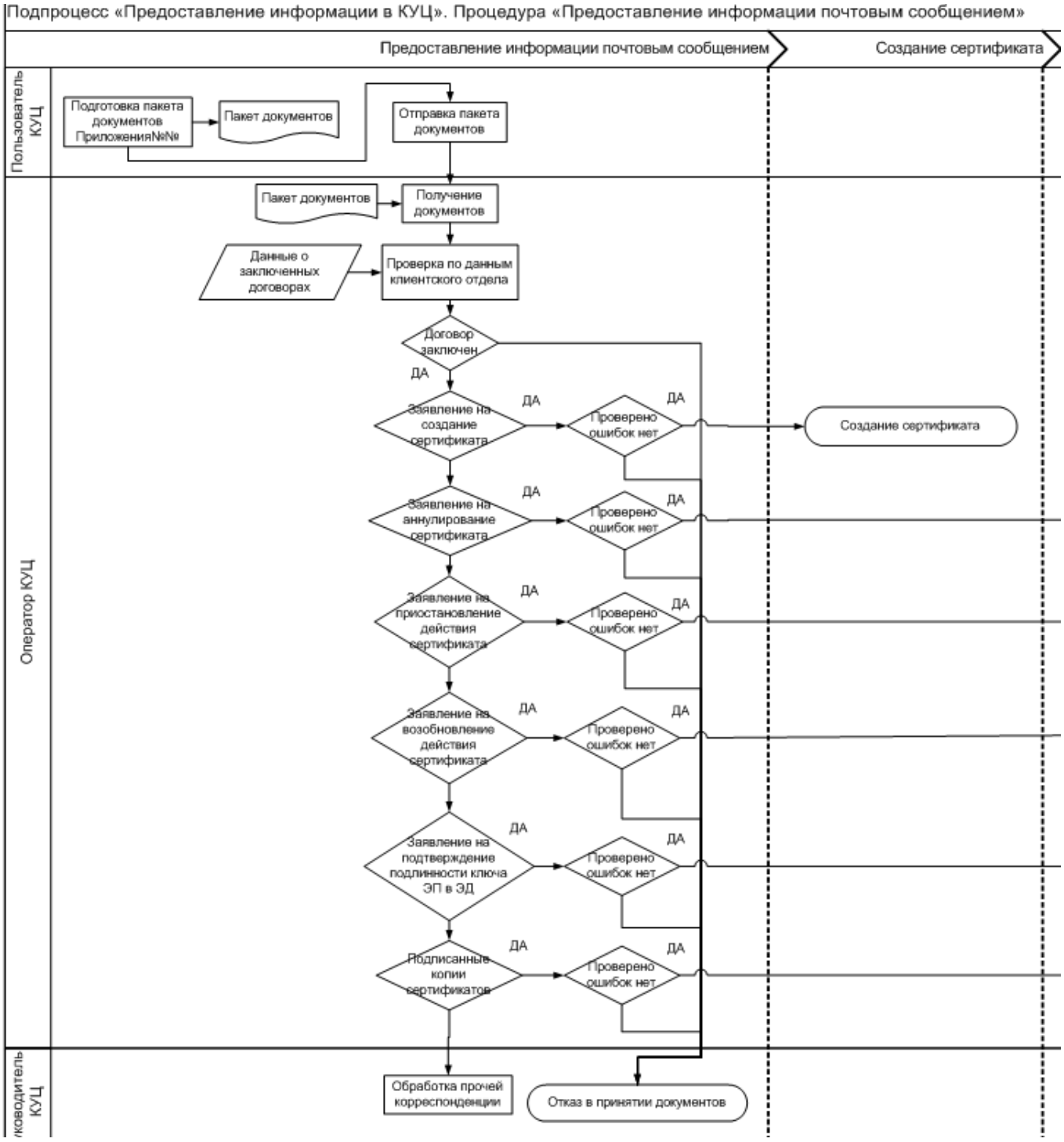


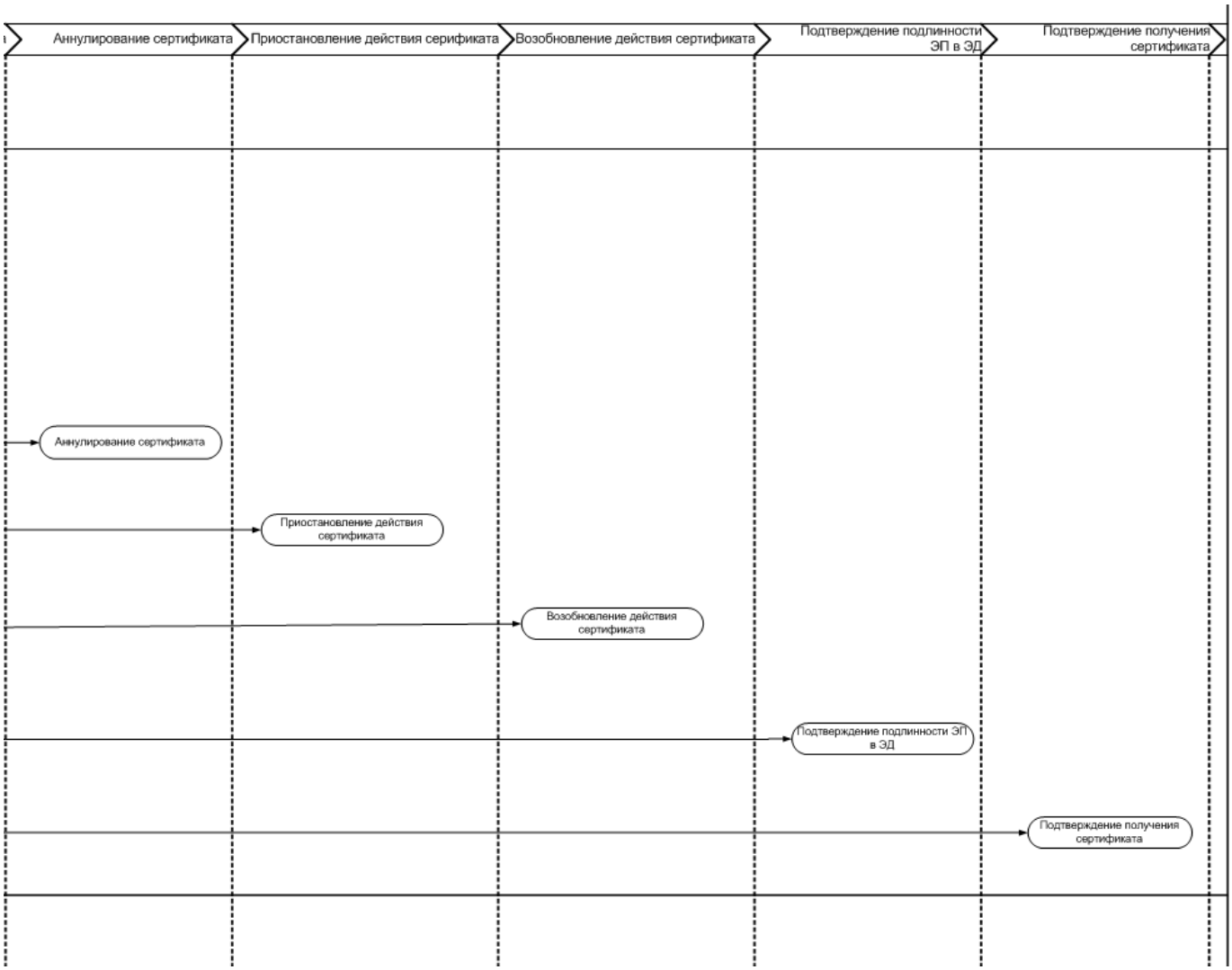
1. Подпроцесс «Предоставление информации в КУЦ»:

а) Схема процедуры «Предоставление информации доверенным лицом»:

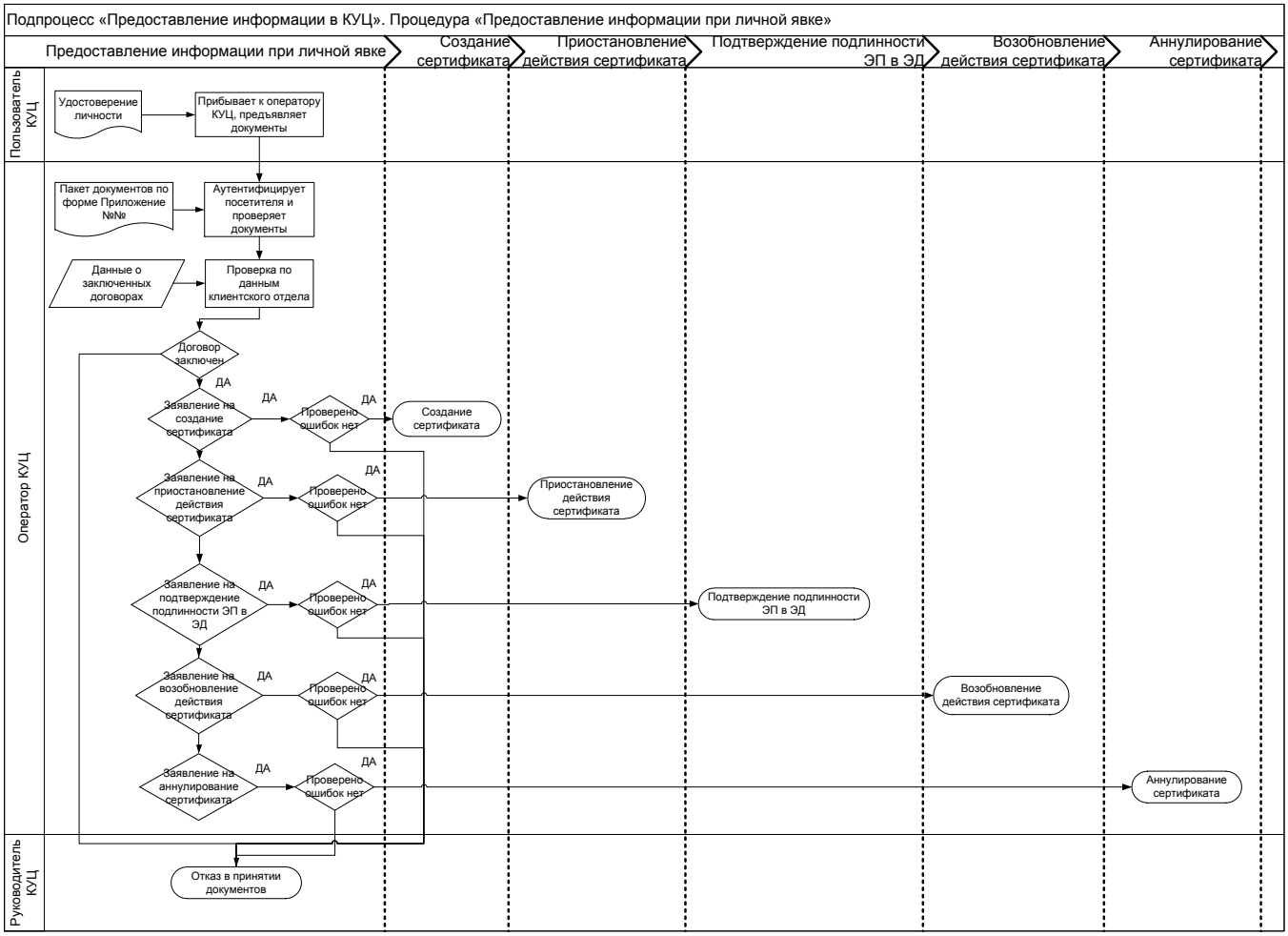


b) Схема процедуры «Предоставление информации почтовым сообщением»:

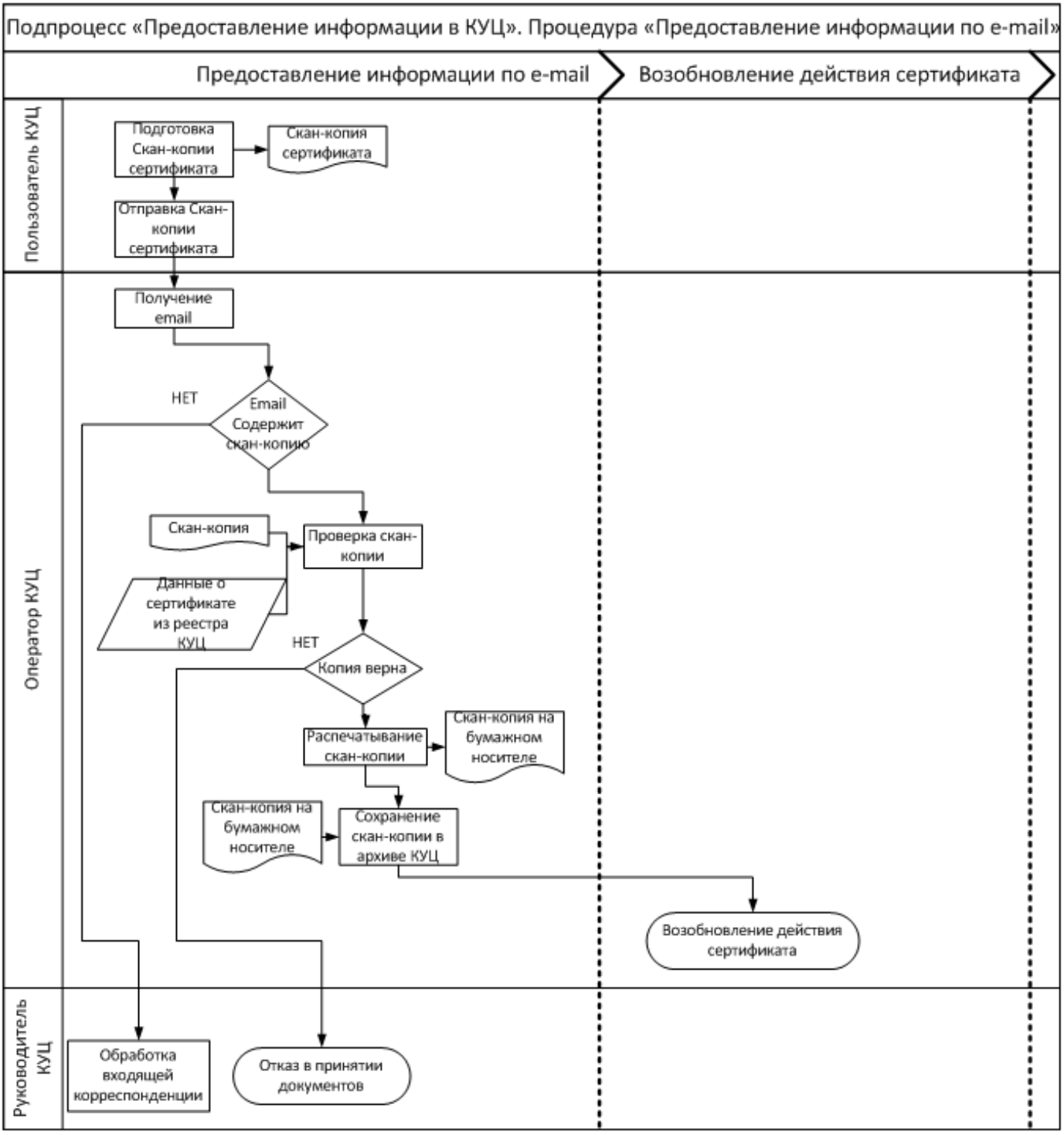



Аннулирование сертификата
Приостановление действия серификата
Возобновление действия сертификата
Подтверждение подлинности ЭП в ЭД
Подтверждение получения сертификата
Аннулирование сертификата
Приостановление действия сертификата
Возобновление действия сертификата
Подтверждение подлинности ЭП в ЭД
Подтверждение получения сертификата

c) Схема процедуры «Предоставление информации при личной явке»:

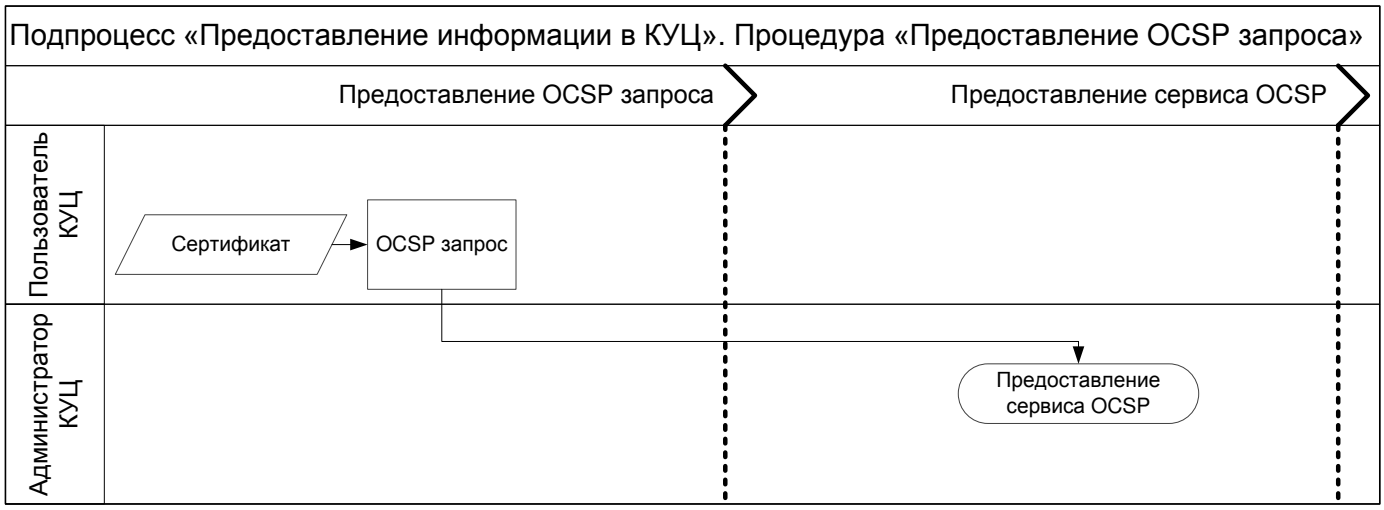


d) Схема процедуры « Предоставление информации по e-mail»:

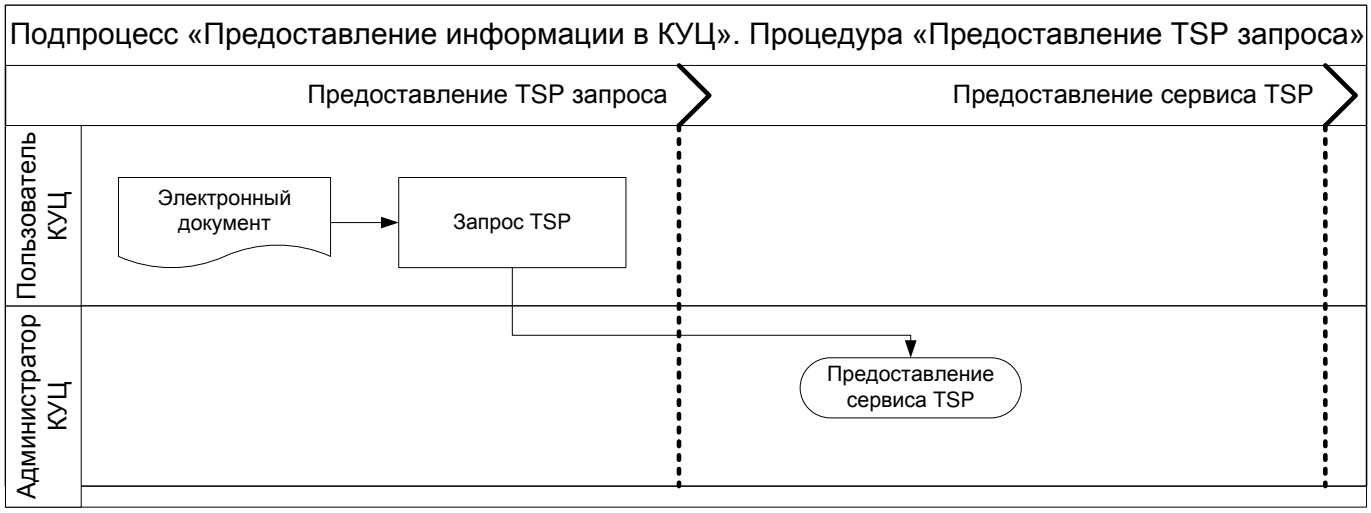


е) Схема процедуры «Предоставление информации по телефону»:

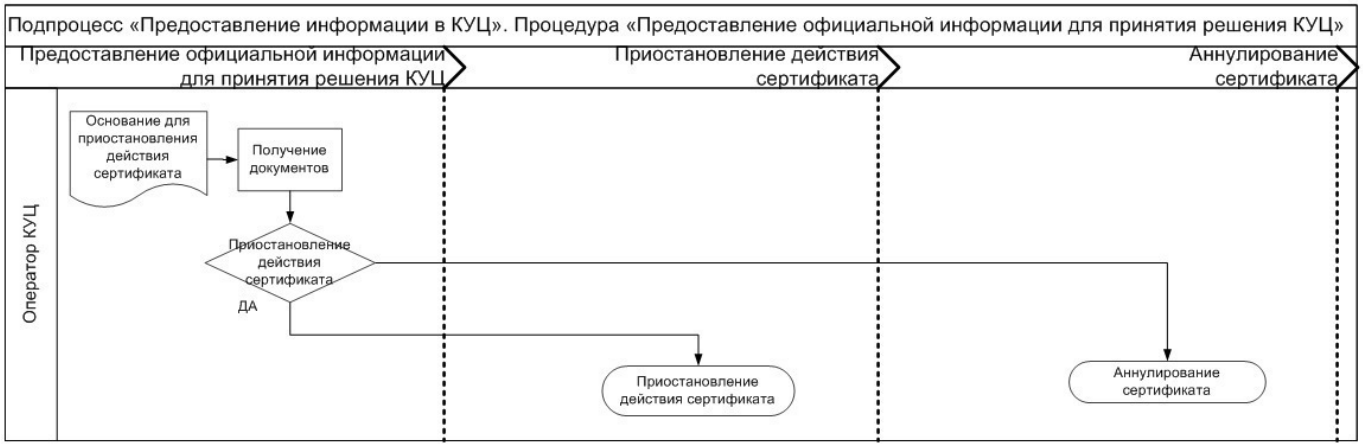
f) Схема процедуры «Предоставление OCSP запроса»:



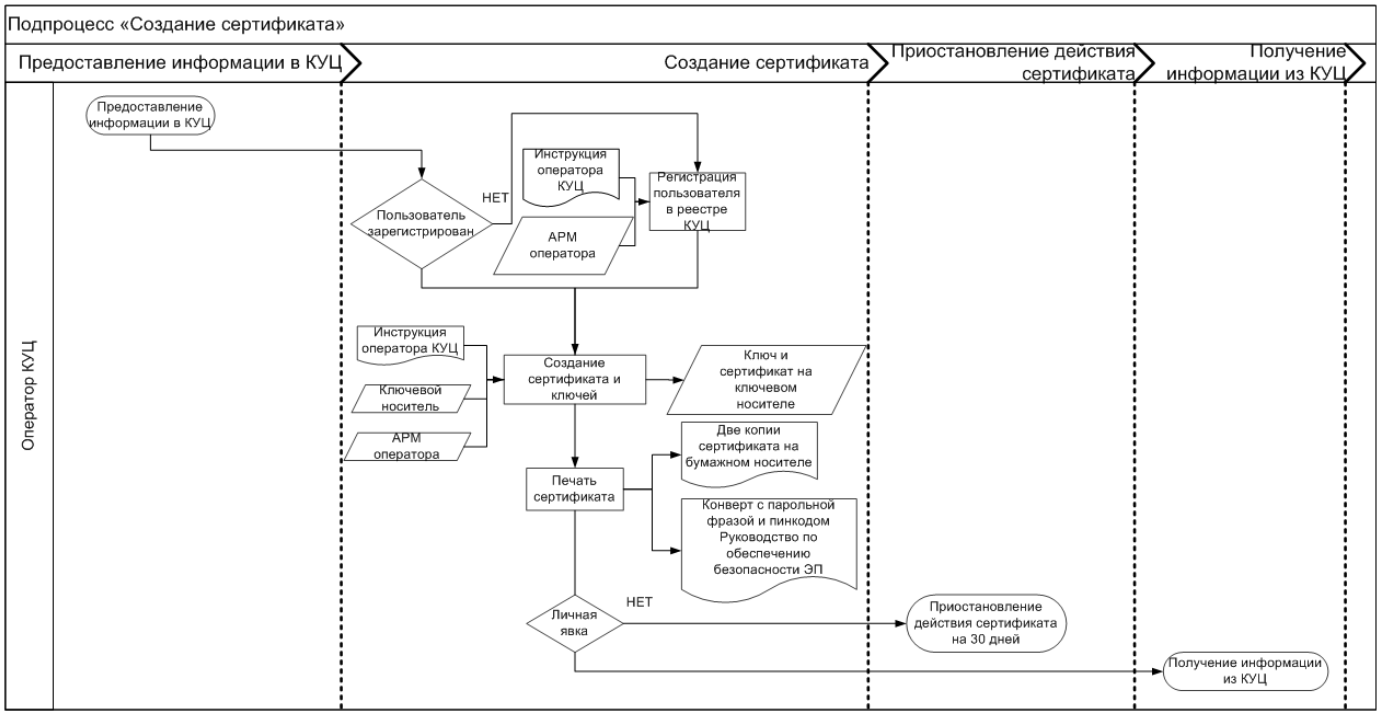
g) Схема процедуры «Предоставление TSP запроса»:



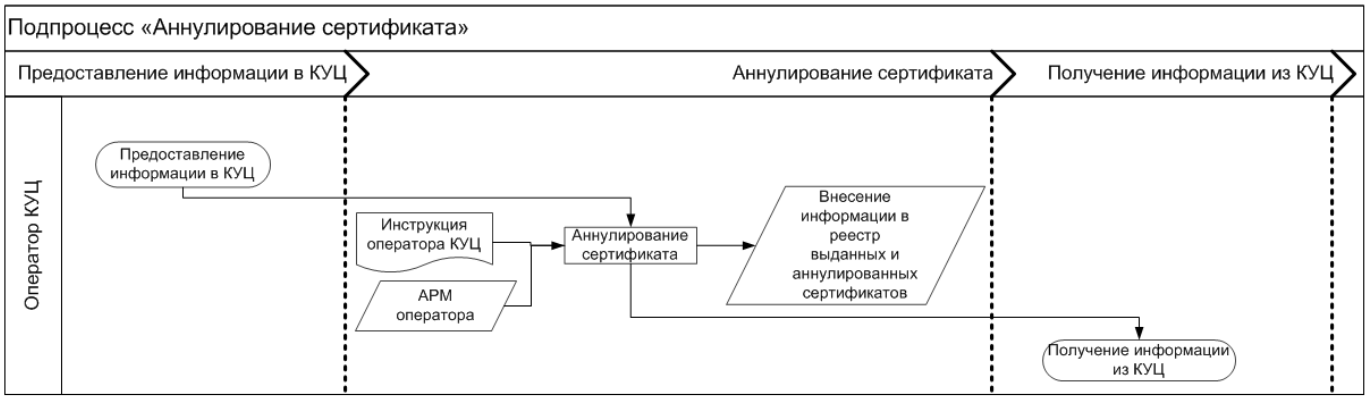
h) Схема процедуры «Предоставление официальной информации для принятия решения КУЦ»:



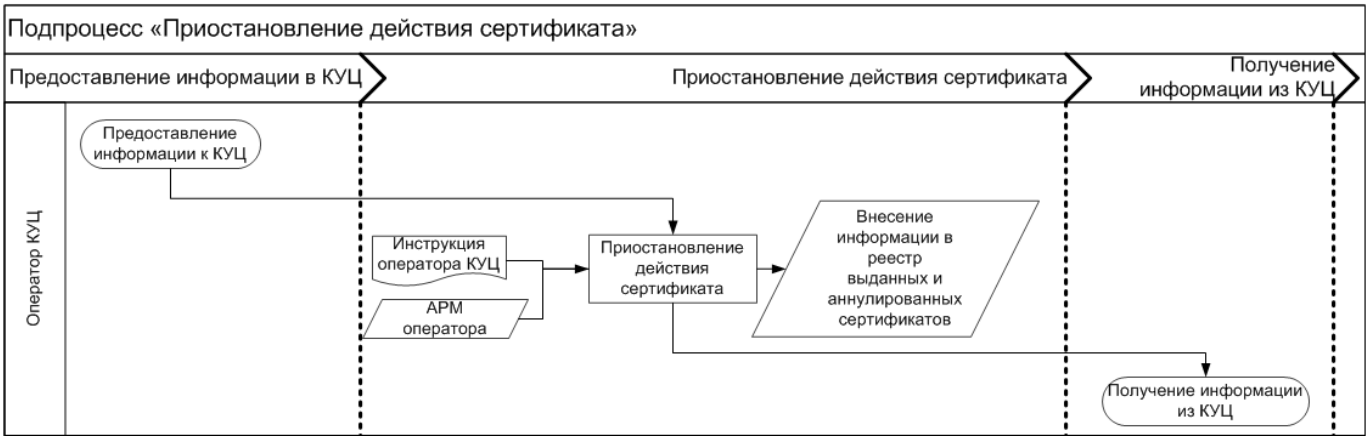
2. Схема подпроцесса «Создание сертификата»:



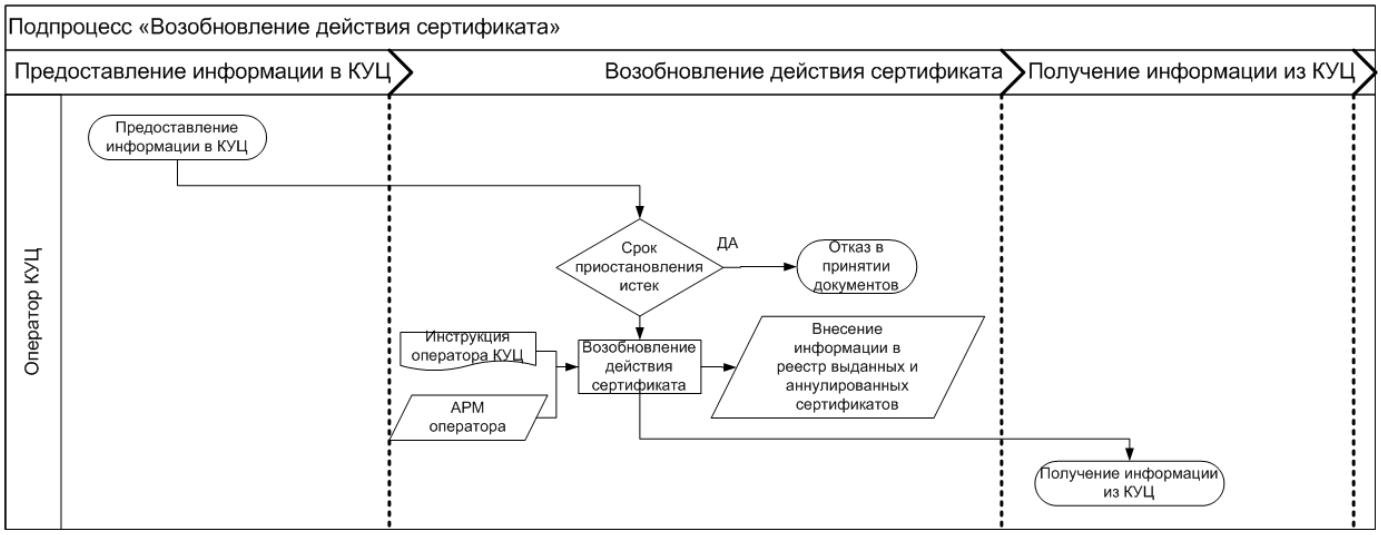
3. Схема подпроцесса «Аннулирование сертификата»:



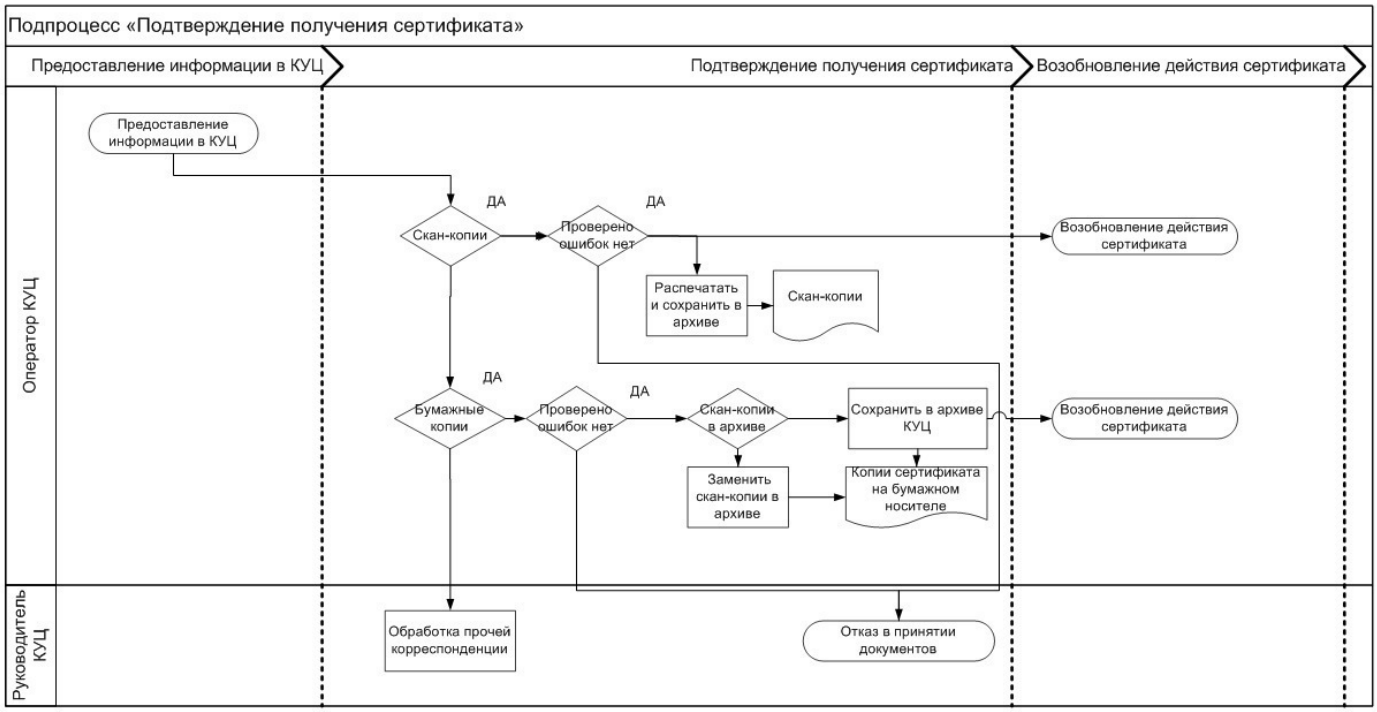
4. Схема подпроцесса «Приостановление действия сертификата»:



5. Схема подпроцесса «Возобновление действия сертификата»:

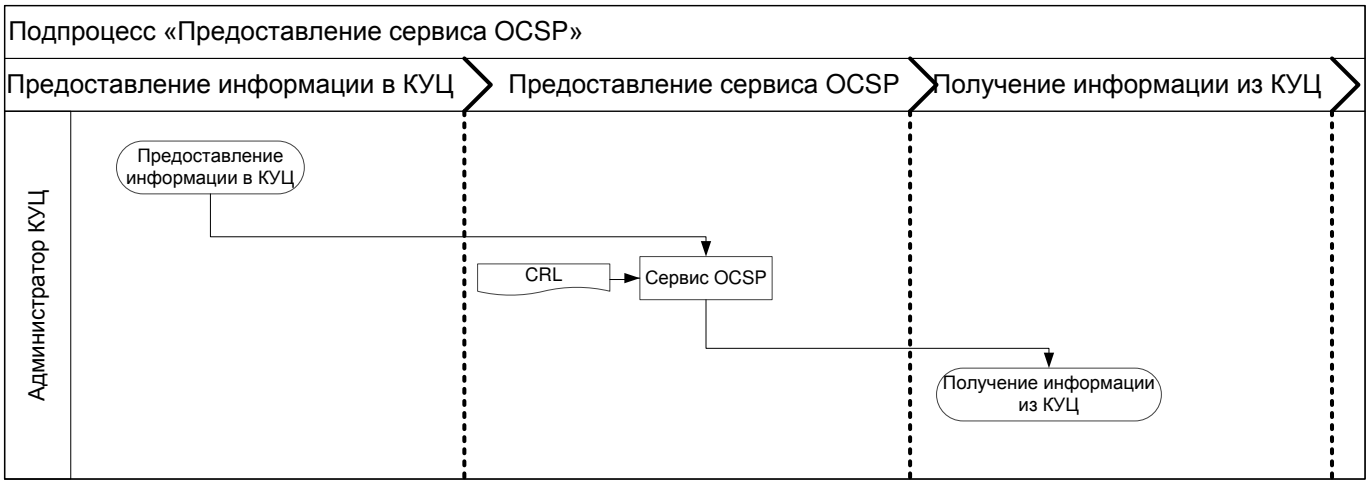


6. Схема подпроцесса «Подтверждение получения сертификата»:

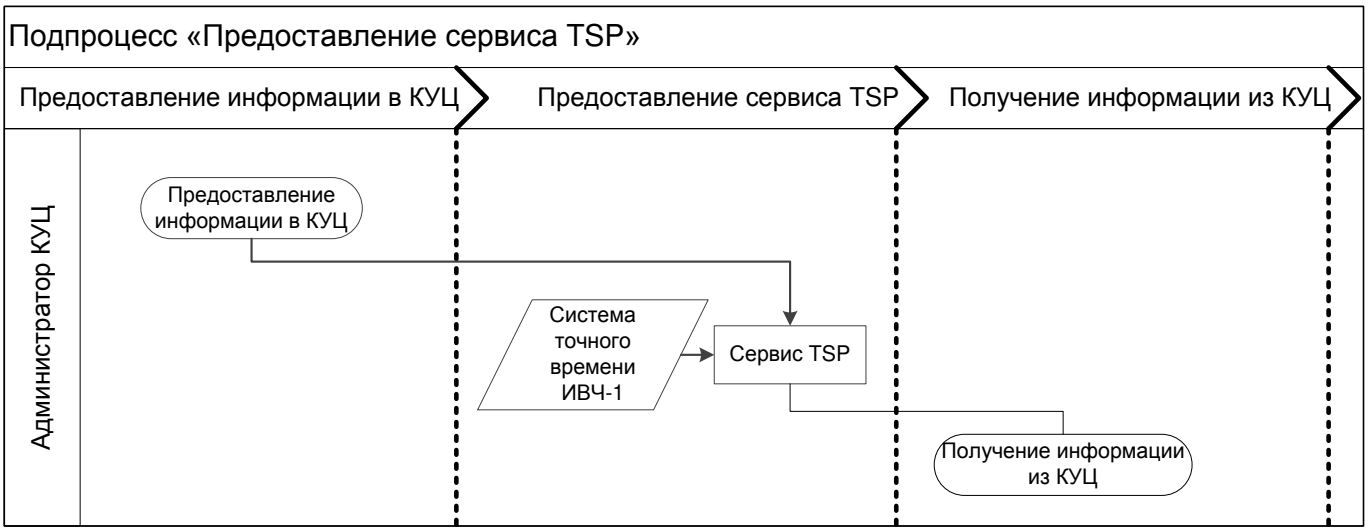


7. Схема подпроцесса «Подтверждение подлинности ЭП в ЭД»:

8. Схема подпроцесса «Предоставление сервиса OCSP»:

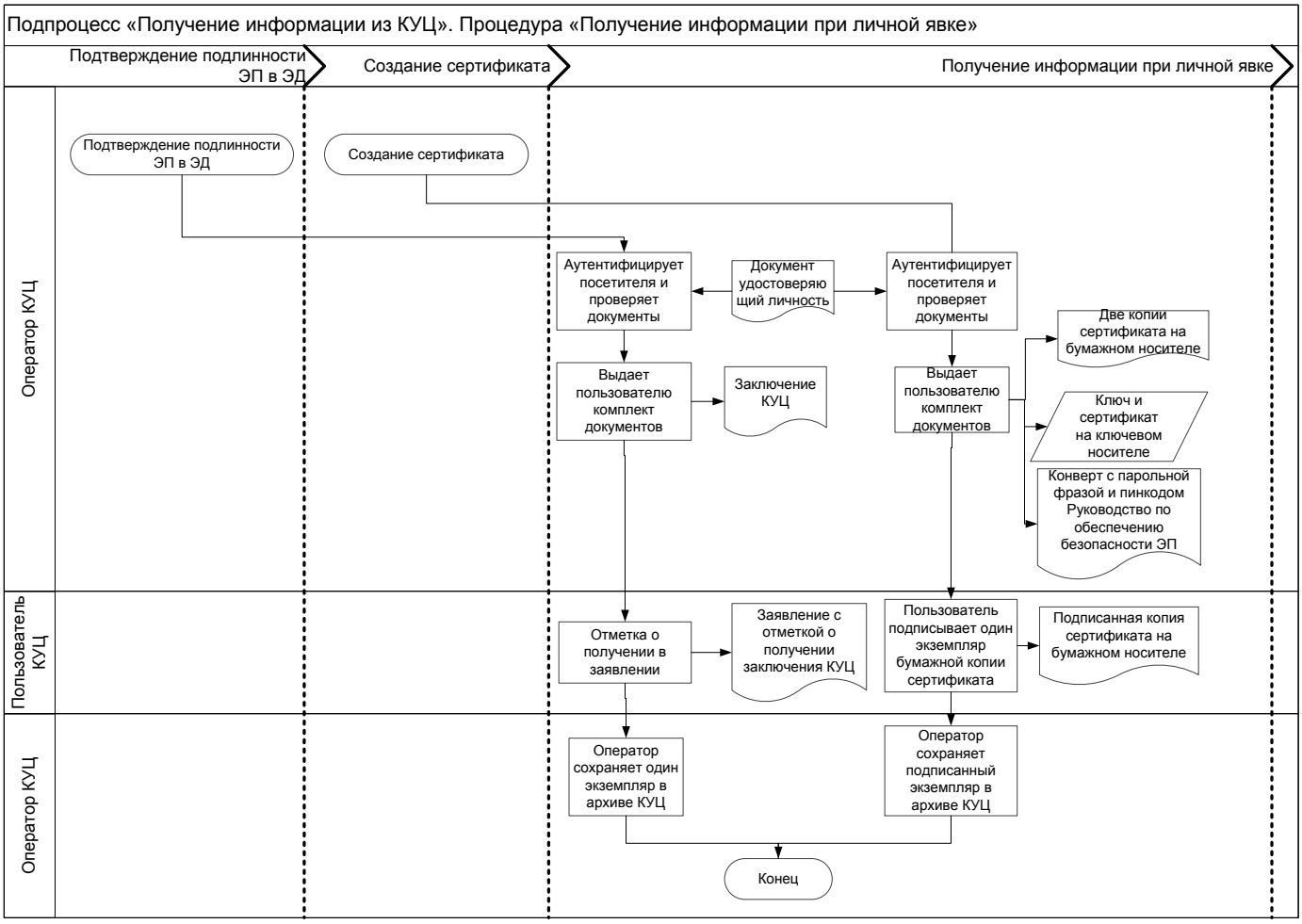


9. Схема подпроцесса «Предоставление сервиса TSP»:

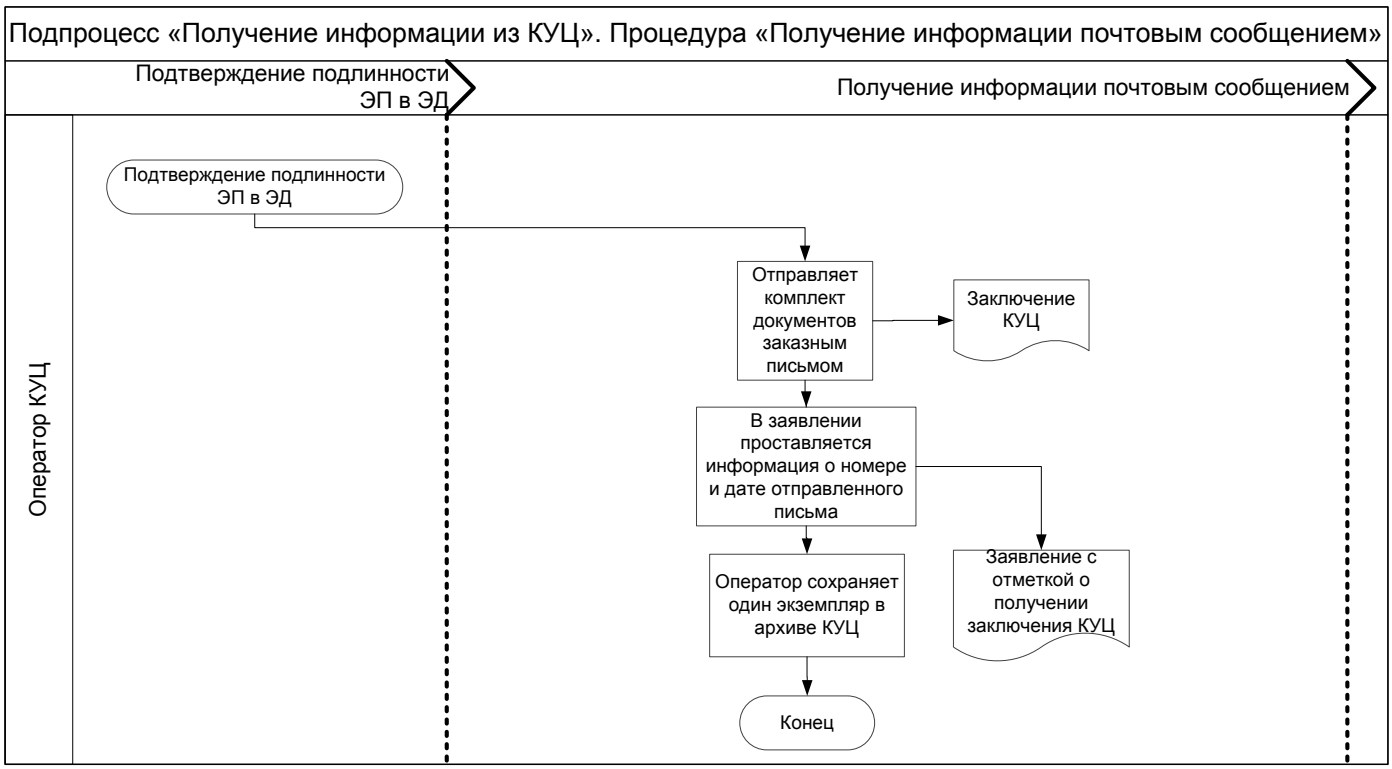


10.Подпроцесс «Получение информации из КУЦ»:

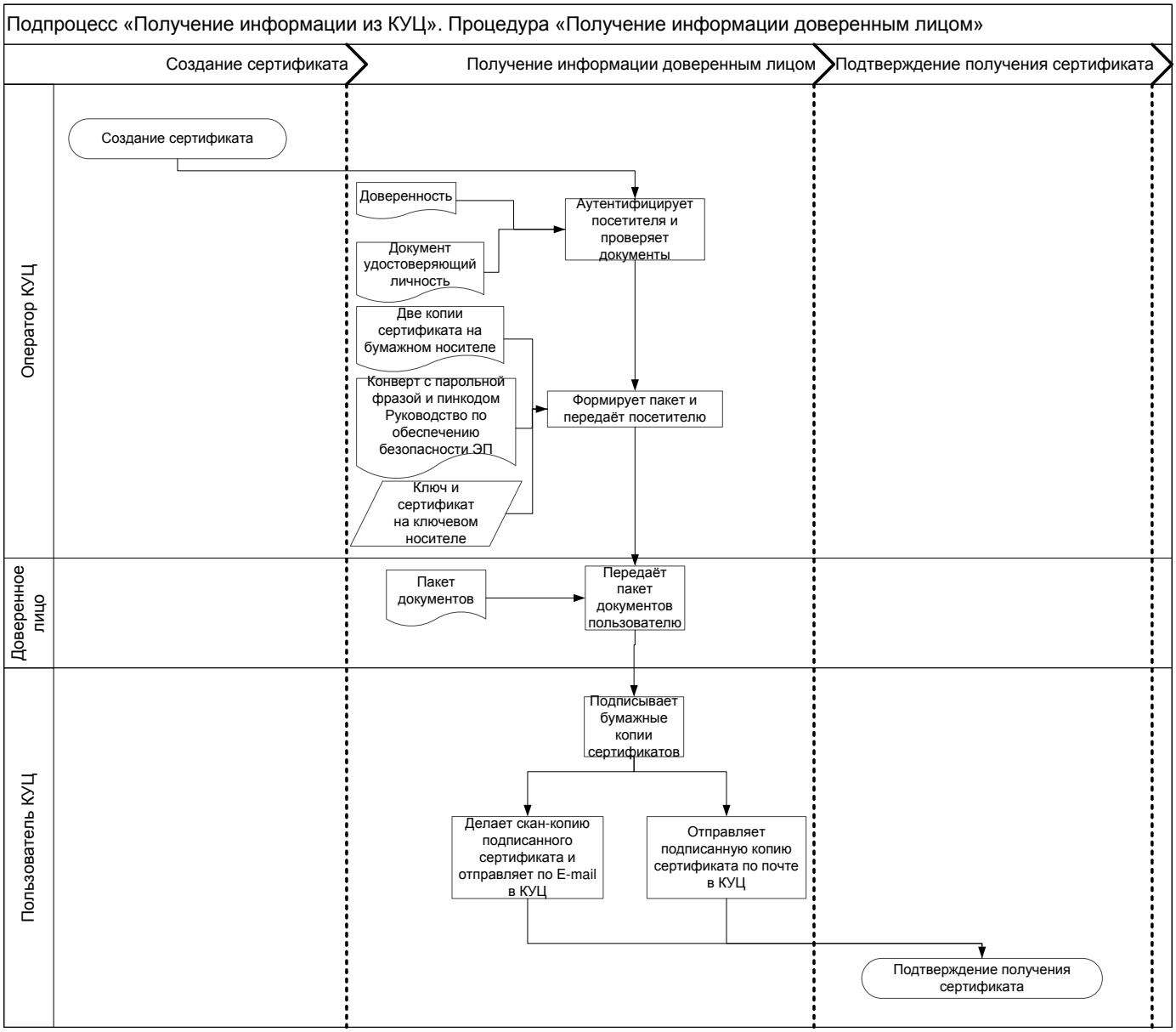
а) Схема процедуры «Получение информации при личной явке»:



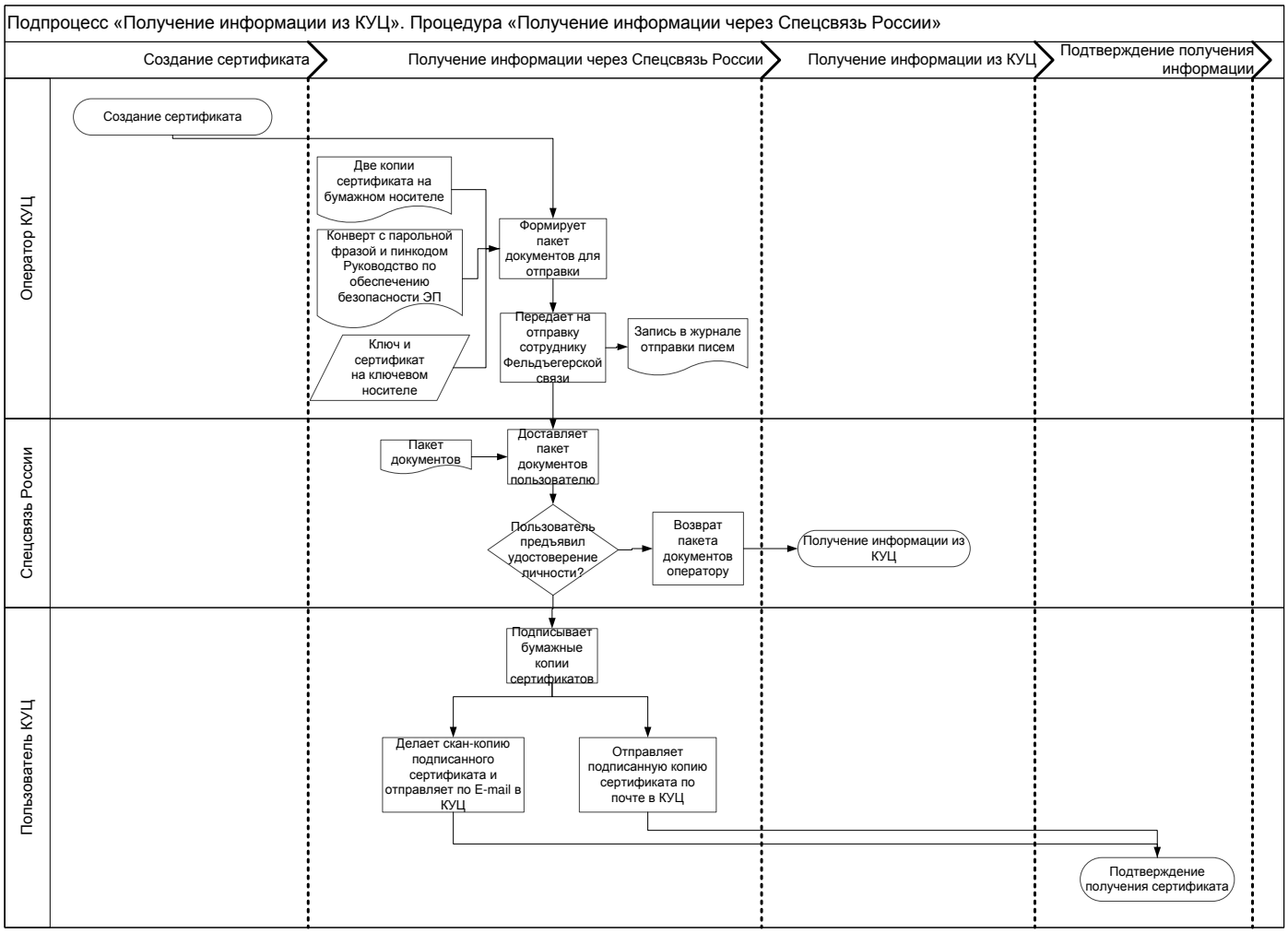
b) Схема процедуры «Получение информации почтовым сообщением»:



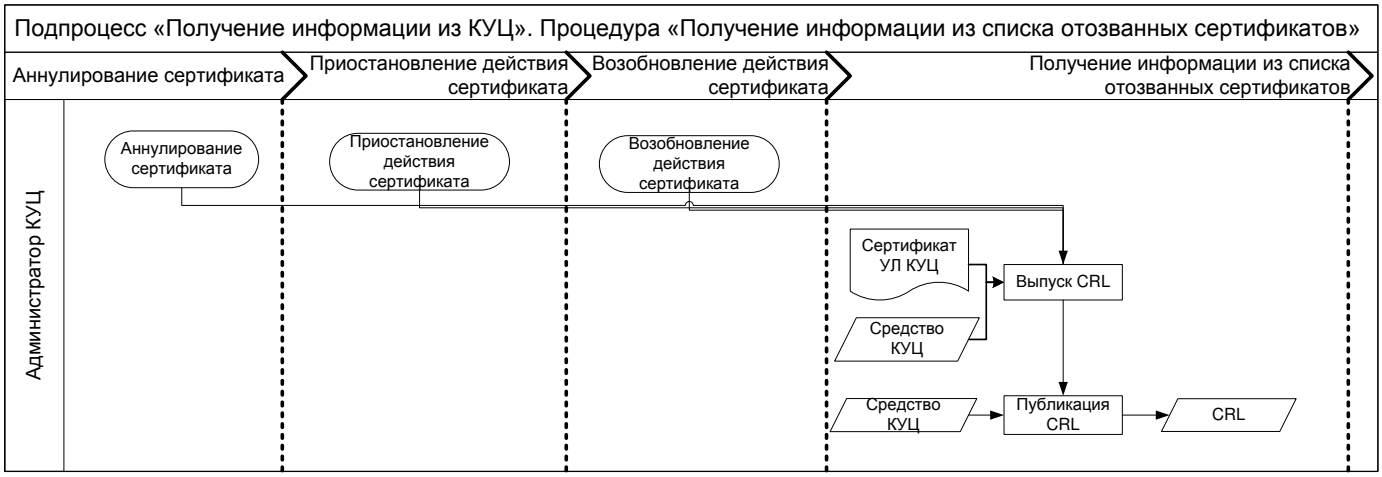
c) Схема процедуры «Получение информации доверенным лицом»:



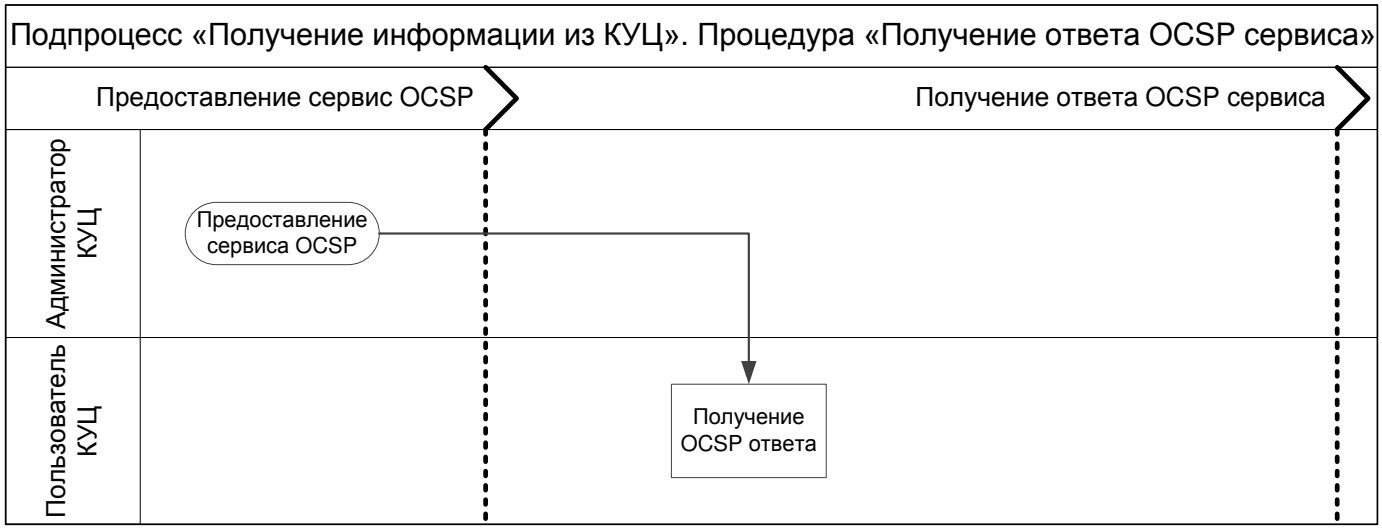
d) Схема процедуры «Получение информации через Спецсвязь России»:



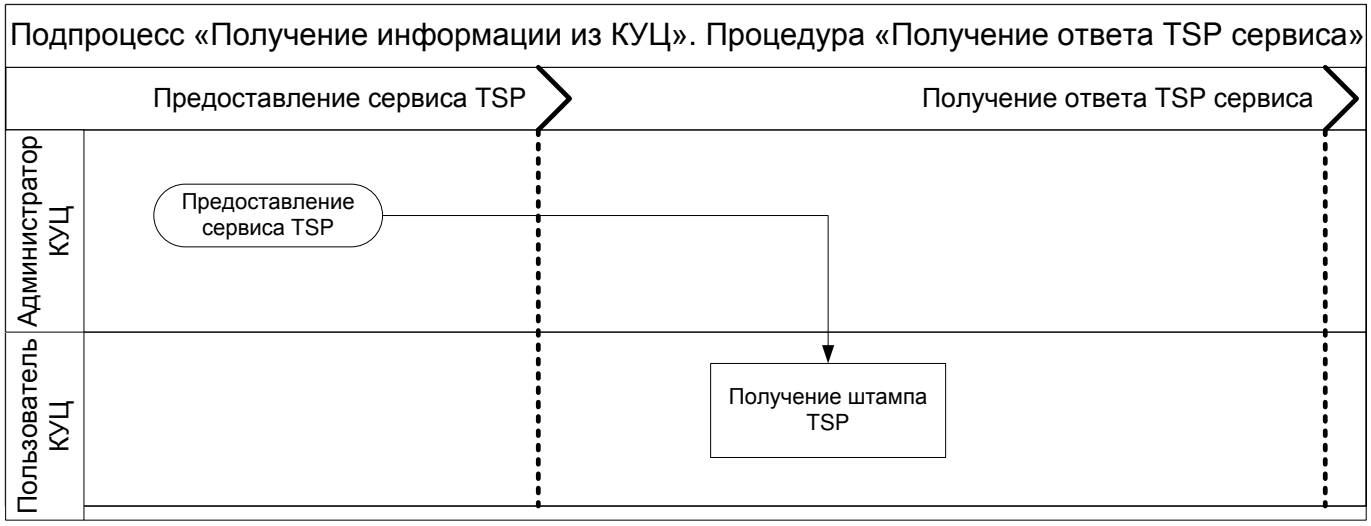
e) Схема процедуры «Получение информации из списков отозванных сертификатов»:



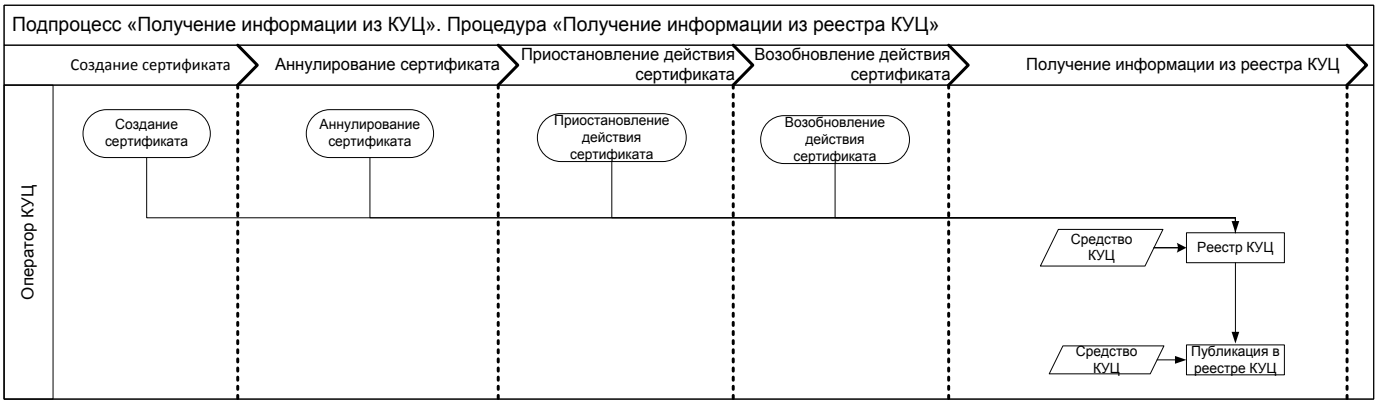
f) Схема процедуры «Получение ответа OCSP сервиса»:



g) Схема процедуры «Получение ответа TSP сервиса»:



h) Схема процедуры «Получение информации из реестра КУЦ»:



Приложение №3

Дополнительные выходы и дополнительные входы

№ подпроцесса	Наименование дополнительного выхода процесса	Потребитель дополнительного выхода процесса (группа процессов/ внешний контрагент)
1	Информация о выданных сертификатах	АО «Гринатом»

№ п/п	Наименование дополнительного входа процесса	Поставщик дополнительного входа процесса (группа процессов/ внешний контрагент)
1	Информация о заключенных договорах	АО «Гринатом»

Приложение №4

Заявление на создание квалифицированного сертификата ключа проверки электронной подписи

«_____» _____ 201__г.

_____

наименование организации, включая организационно-правовую форму

в лице _____

должность

_____

_фамилия, имя, отчество

действующего на основании _____

просит:

1. создать квалифицированный сертификат ключа проверки электронной подписи (далее - сертификат) содержащий следующие данные:

Наименование	Длина	Значение
Общее имя	64	
Организация	64	
Адрес (ул., дом)	30	
Населённый пункт	128	
Регион	128	
ИНН	12	
ОГРН	13	
Страна	2	RU

2. В качестве владельца сертификата наряду с указанием в сертификате наименования нашей организации прошу указать следующего полномочного представителя, действующего от имени нашей организации и внести в сертификат следующие данные:

Наименование	Длина	Значение	
Фамилия	40		
Имя Отчество	64		
Должность	64		
Подразделение	64		
Email	128		
СНИЛС	11		
Уч. запись в домене GK			@gk.rosatom.local

3. Указать область ограничения использования сертификата:

4. Предоставить ключевой носитель и сертификат (отметить галочкой):

В Корпоративном удостоверяющем центре по адресу:	
Службой специальной связи по адресу (указать адрес и имя получателя):	

Владелец сертификата соглашается с обработкой своих персональных данных АО «Гринатом» и признает, что персональные данные, заносимые в сертификаты ключей проверки электронной подписи, относятся к общедоступным персональным данным.

Владелец сертификата ключа проверки электронной подписи _____/_____/

(подпись) (ФИО)

Уполномоченное должностное лицо

_____ _____/_____/

(Должность) (подпись) (ФИО)

М.П.

Приложение № 5

Правила заполнения заявлений на создание сертификатов ключей проверки электронной подписи

Правила заполнения заявлений на создание квалифицированного сертификатов ключа проверки электронной подписи

1. Общие положения

1.1. Настоящие Правила определяют порядок формирования запросов и оформление заявлений на создание квалифицированного сертификата ключа проверки электронной подписи (далее - сертификата), направляемого в удостоверяющий центр.

1.2. В части настоящих Правил определены форматы заполнения основных атрибутов, содержащихся в заявлении на сертификат: C, SN, GN, Street, S, L, O, OU, T, CN, E (в соответствии со стандартом x.509), дополнительных атрибутов: ИНН, ОГРН, СНИЛС, а также требования к оформлению заявлений на создание сертификата.

1.3. Наименование атрибутов с использованием букв латинского алфавита допускается только в случаях, когда наименование атрибута на русском языке отсутствует.

1.4. Каждое слово в поле должно быть отделено ровно одним пробелом.

1.5. Не разрешается использовать пробел в начале и в конце текста.

1.6. Необходимо использовать заглавные и строчные буквы так, как это продиктовано правилами русского языка.

1.7. При нарушении данных правил в выдаче сертификата может быть отказано.

2. Правила заполнения полей заявления на создание сертификата

Заявление на создание квалифицированного сертификата содержит две таблицы. Первая таблица содержит данные об организации:

№ п.п.	Наименование	Длина	Поле сертификата
1.	Общее имя	64	CN
2.	Организация	64	O
3.	Адрес (ул., дом)	30	Street
4.	Населённый пункт	128	L
5.	Регион	128	S
6.	ИНН	12	INN
7.	ОГРН	13	OGRN
8.	Страна	2	C

2.1. Формат поля Общее имя

– В атрибуте CN субъекта сертификата записываются фамилия, имя, отчество для физического лица или наименование организации – для юридического лица, атрибут является обязательным.

– В случае выпуска сертификата для аутентификации сервера в поле CN указывается полное доменное имя сервера.

– При выпуске сертификата для тестовых целей в поле CN указывается запись обозначающая цели сертификата (например - «Для тестовых целей» или «Тестовый сертификат»).

– Длина текста – не более 64 символов.

2.2. Формат названия организации владельца сертификата.

– Название организации владельца сертификата записывается в атрибут «O» субъекта сертификата, атрибут является обязательным для владельцев сертификата – физических лиц - представителей юридического лица.

– Длина текста – не более 64 символов. В случае если длина полного названия организации превышает 64 символа, следует указывать официальное краткое наименование организации. Если официальное краткое наименование отсутствует или его длина превышает 64 символа, следует использовать сокращённое наименование от полного официального наименования. Информация о сокращении подаётся в удостоверяющий центр в виде официального письма.

– Кавычки, точки и прочие знаки пунктуации разрешается использовать только в том случае, если они встречаются внутри официального названия организации.

2.3. Формат адреса организации владельца сертификата.

– Название адреса, где зарегистрирована организация владельца, записывается в атрибут Street субъекта сертификата, атрибут является обязательным.

– Длина текста – не более 30 символов.

– Адрес указывается в виде наименования улицы, номера дома, корпуса, строения, квартиры, помещения (если имеется).

– Кавычки, точки и прочие знаки пунктуации разрешается использовать только в том случае, если они встречаются внутри официального названия адреса.

– Допускается использование общепринятых сокращений из таблицы в п.6.1.

2.4. Формат названия населённого пункта.

– Название населённого пункта, где зарегистрирована организация владельца сертификата, записывается в атрибут L субъекта сертификата, атрибут является обязательным.

– Длина текста – не более 128 символов.

– Вид населённого пункта указывается в начале текста без сокращения.

– Кавычки, точки и прочие знаки пунктуации разрешается использовать только в том случае, если они встречаются внутри официального названия населённого пункта.

2.5. Формат названия региона (области).

– Название региона, где зарегистрировано юридическое лицо владелец сертификата записывается в атрибут «S» субъекта сертификата, атрибут является обязательным. Название региона допускается не заполнять только в случае, если значение Атрибута «L» (см. п.2.7) «Город Москва» или «Город Санкт-Петербург».

– Длина текста – не более 128 символов.

– Разрешается использовать только наименования из таблицы в п.6.2:

– Разрешается использовать наименование, отличное от указанного в таблице в п.6.2, в случае изменения наименований регионов Российской Федерации, а также в том случае, если сертификат будет выдаваться на нерезидента Российской Федерации.

2.6. Формат ИНН.

– Идентификационный номер налогоплательщика - юридического лица.

– Текст длиной 10 цифр для юридического лица или 12 цифр для индивидуального предпринимателя и физического лица.

– Атрибут является обязательным.

– Разрешено использовать только цифровые символы 0123456789.

– Запрещено использование ИНН, не проходящих проверку корректности на контрольные разряды.

2.7. Формат ОГРН. Основной государственный регистрационный номер юридического лица.

– Текст длиной 13 цифр - только для юридического лица.

– Атрибут является обязательным.

– Разрешено использовать только цифровые символы 0123456789.

– Запрещено использование ОГРН, не проходящих проверку корректности на контрольные разряды.

2.8. Формат названия страны

– Название страны, где зарегистрирована организация владельца сертификата, записывается в атрибут C субъекта сертификата, атрибут является обязательным.

– Длина текста – не более 2 символов.

– В поле название страны для организации, зарегистрированных на территории Российской Федерации указывается значение «RU»

3. Правила заполнения полей владельца сертификата.

Вторая таблица в заявлении на создание сертификата содержит данные о владельце сертификата:

№ п.п.	Наименование	Длина	Поле сертификата
1.	Фамилия	40	SN
2.	Имя Отчество	64	GN
3.	Должность	64	T
4.	Подразделение	64	OU
5.	Email	128	E
6.	СНИЛС	11	SNILS
7.	Уч. запись в домене GK		UPN

3.1. Формат фамилии владельца сертификата владельца

– Фамилия сертификата записываются в атрибут SN субъекта сертификата

– Атрибут является не обязательным.

– Длина текста – не более 40 символов.

– При выпуске сертификата для тестовых целей в поле SN либо не заполняются, либо содержит информацию о тестовых целях сертификата. (например – «Для тестовых целей» или «Тест»)

– При выпуске сертификата аутентификации сервера поля SN не заполняется

3.2. Формат Имя и отчества владельца сертификата владельца

– Имя и отчество владельца сертификата записываются в атрибут GN субъекта сертификата к, атрибут является не обязательным.

– Длина текста – не более 64 символов.

– При выпуске сертификата для тестовых целей в поле GN либо не заполняются, либо содержит информацию о тестовых целях сертификата. (например – «Для тестовых целей» или «Тест»)

– При выпуске сертификата аутентификации сервера поле GN не заполняется.

3.3. Формат должности владельца сертификата.

– Должность владельца сертификата записывается в атрибут «T» субъекта сертификата, атрибут не является обязательным.

– Длина текста – не более 64 символов.

– Кавычки, точки и прочие знаки пунктуации разрешается использовать только в том случае, если они встречаются внутри официального названия должности.

3.4. Формат подразделения организации владельца сертификата.

– Подразделение организации владельца сертификата записывается в атрибут OU субъекта сертификата, атрибут не является обязательным.

– Длина текста – не более 64 символов.

– Кавычки, точки и прочие знаки пунктуации разрешается использовать только в том случае, если они встречаются внутри официального названия подразделения организации.

3.5. Формат адреса электронной почты владельца сертификата.

– Адрес электронной почты владельца сертификата записывается в атрибут E субъекта сертификата.

– Длина текста – не более 128 символов.

– При заполнении адреса электронной почты необходимо руководствоваться правилами, определёнными в стандарте текстовых сообщений Internet RFC 822.

– Разрешается указывать только реальный адрес электронной почты.

3.6. Формат СНИЛС. Страховой номер индивидуального лицевого счёта физического лица.

– Текст длиной 14 символов - только для физического лица

– Атрибут является обязательным.

– Разрешено использовать только цифровые символы 0123456789.

– Запрещено использование СНИЛС, не проходящих проверку корректности на контрольные разряды.

3.7. Формат учётной записи в домене GK

– В поле «Информация об учётной записи пользователя в домене GK (при необходимости доступа к Корпоративным информационным системам)» указывается имя учётной записи пользователя в виде IOFamily@gk.rosatom.local

– В одном сертификате может содержаться только одно имя учётной записи пользователя.

– Имя учётной записи пользователя вносится в поле сертификата «Дополнительное имя субъекта (SubjectAlternaiveName)» в поле UPN (UserPrincipalName) и должно совпадать с полем UPN учётной записи пользователя в корпоративном домене GK.

4. Правила заполнения области ограничения использования квалифицированного сертификата.

Поле «область ограничения использования квалифицированного сертификата» должно быть выбрано в соответствии с шаблоном сертификата в соответствии с Приложением №6

5. Правила заполнения способа доставки ключевого носителя и сертификата.

– Должен быть выбран один из способов доставки ключевого носителя и сертификата.

– При выборе доставки Службой специальной связи в заявлении долен быть указан адрес доставки в следующем виде: Регион (область, край, республика), Населённый пункт (город, посёлок, и т.д.), Название организации, Адрес (улица, дом), ФИО получателя

6. Дополнительные положения.

6.1. Таблица 1 - Сокращения адреса

Сокращение	Название
ул.	улица
пр-т	проспект
пр-д	проезд
пер.	переулок
наб.	набережная
пл.	площадь
б-р	бульвар

Сокращение	Название
ш.	шоссе
д.	дом
корп.	корпус
стр.	строение
кв.	квартира
п.	помещение

6.2. Таблица 2 - Справочник регионов

Код	Название региона	Код	Название региона
01	Республика Адыгея (Адыгея)	44	Костромская область
02	Республика Башкортостан	45	Курганская область
03	Республика Бурятия	46	Курская область
04	Республика Алтай	47	Ленинградская область
05	Республика Дагестан	48	Липецкая область
06	Республика Ингушетия	49	Магаданская область
07	Кабардино-Балкарская Республика	50	Московская область
08	Республика Калмыкия	51	Мурманская область
09	Карачаево-Черкесская Республика	52	Нижегородская область
10	Республика Карелия	53	Новгородская область
11	Республика Коми	54	Новосибирская область
12	Республика Марий Эл	55	Омская область
13	Республика Мордовия	56	Оренбургская область
14	Республика Саха (Якутия)	57	Орловская область
15	Республика Северная Осетия – Алания	58	Пензенская область
16	Республика Татарстан	59	Пермский край
17	Республика Тыва	60	Псковская область
18	Удмуртская Республика	61	Ростовская область
19	Республика Хакасия	62	Рязанская область
20	Чеченская Республика	63	Самарская область
21	Чувашская Республика – Чувашия	64	Саратовская область
22	Алтайский край	65	Сахалинская область
23	Краснодарский край	66	Свердловская область
24	Красноярский край	67	Смоленская область
25	Приморский край	68	Тамбовская область
26	Ставропольский край	69	Тверская область
27	Хабаровский край	70	Томская область
28	Амурская область	71	Тульская область
29	Архангельская область и Ненецкий автономный округ	72	Тюменская область
30	Астраханская область	73	Ульяновская область
31	Белгородская область	74	Челябинская область
32	Брянская область	75	Забайкальский край
33	Владимирская область	76	Ярославская область
34	Волгоградская область	77	г. Москва
35	Вологодская область	78	г. Санкт-Петербург
36	Воронежская область	79	Еврейская автономная область
37	Ивановская область	86	Ханты-Мансийский автономный округ – Югра
38	Иркутская область	87	Чукотский автономный округ
39	Калининградская область	89	Ямало-Ненецкий автономный округ
40	Калужская область	91	Республика Крым
41	Камчатский край	92	г. Севастополь
42	Кемеровская область	99	Иные территории, включая, г. Байконур
43	Кировская область		

6.3. Набор разрешённых символов в запросе на сертификат.

– При использовании в тексте полей сертификата символов UNICODE, коды которых не указаны в таблице 3, в выдаче сертификата может быть отказано.

Таблица 3 - Разрешённые символы

№	Символ	Название			
1		пробел	74	w	латинская строчная буква w
2	"	универсальная кавычка	75	x	латинская строчная буква x
3	%	процент	76	y	латинская строчная буква y
4	&	амперсанд	77	z	латинская строчная буква z
5	'	апостроф	78	Ё	кириллическая заглавная буква Ё
6	(	левая скобка	79	«	двойная левая угловая кавычка
7	)	правая скобка	80	ё	кириллическая строчная буква ё
8	+	знак плюс	81	№	знак номер
9	,	запятая	82	»	двойная правая угловая кавычка
10	-	дефис	83	А	кириллическая заглавная буква А
11	,	точка	84	Б	кириллическая заглавная буква Б
12	0	цифра ноль	85	В	кириллическая заглавная буква В
13	1	цифра один	86	Г	кириллическая заглавная буква Г
14	2	цифра два	87	Д	кириллическая заглавная буква Д
15	3	цифра три	88	Е	кириллическая заглавная буква Е
16	4	цифра четыре	90	Ж	кириллическая заглавная буква Ж
17	5	цифра пять	91	З	кириллическая заглавная буква З
18	6	цифра шесть	92	И	кириллическая заглавная буква И
19	7	цифра семь	93	Й	кириллическая заглавная буква Й
20	8	цифра восемь	94	К	кириллическая заглавная буква К
21	9	цифра девять	95	Л	кириллическая заглавная буква Л
22	:	двоеточие	96	М	кириллическая заглавная буква М
23	;	точка с запятой	97	Н	кириллическая заглавная буква Н
24	@	коммерческое ат «собачка»	98	О	кириллическая заглавная буква О
25	A	латинская заглавная буква A	99	П	кириллическая заглавная буква П
26	B	латинская заглавная буква B	100	Р	кириллическая заглавная буква Р
27	C	латинская заглавная буква C	101	С	кириллическая заглавная буква С
28	D	латинская заглавная буква D	102	Т	кириллическая заглавная буква Т
29	E	латинская заглавная буква E	103	У	кириллическая заглавная буква У
30	F	латинская заглавная буква F	104	Ф	кириллическая заглавная буква Ф
31	G	латинская заглавная буква G	105	Х	кириллическая заглавная буква Х
32	H	латинская заглавная буква H	106	Ц	кириллическая заглавная буква Ц
33	I	латинская заглавная буква I	107	Ч	кириллическая заглавная буква Ч
34	J	латинская заглавная буква J	108	Ш	кириллическая заглавная буква Ш
35	K	латинская заглавная буква K	109	Щ	кириллическая заглавная буква Щ
36	L	латинская заглавная буква L	110	Ъ	кириллическая заглавная буква Ъ
37	M	латинская заглавная буква M	111	Ы	кириллическая заглавная буква Ы
38	N	латинская заглавная буква N	112	Ь	кириллическая заглавная буква Ь
39	O	латинская заглавная буква O	113	Э	кириллическая заглавная буква Э
40	P	латинская заглавная буква P	114	Ю	кириллическая заглавная буква Ю
41	Q	латинская заглавная буква Q	115	Я	кириллическая заглавная буква Я
42	R	латинская заглавная буква R	116	а	кириллическая строчная буква а
43	S	латинская заглавная буква S	117	б	кириллическая строчная буква б
44	T	латинская заглавная буква T	118	в	кириллическая строчная буква в
45	U	латинская заглавная буква U	119	г	кириллическая строчная буква г

46	V	латинская заглавная буква V	120	д	кириллическая строчная буква д
47	W	латинская заглавная буква W	121	е	кириллическая строчная буква е
48	X	латинская заглавная буква X	122	ж	кириллическая строчная буква ж
49	Y	латинская заглавная буква Y	123	з	кириллическая строчная буква з
50	Z	латинская заглавная буква Z	124	и	кириллическая строчная буква и
51	_	подчеркивание	125	й	кириллическая строчная буква й
52	a	латинская строчная буква a	126	к	кириллическая строчная буква к
53	b	латинская строчная буква b	127	л	кириллическая строчная буква л
54	c	латинская строчная буква c	128	м	кириллическая строчная буква м
55	d	латинская строчная буква d	129	н	кириллическая строчная буква н
56	e	латинская строчная буква e	130	о	кириллическая строчная буква о
57	f	латинская строчная буква f	131	п	кириллическая строчная буква п
58	g	латинская строчная буква g	132	р	кириллическая строчная буква р
59	h	латинская строчная буква h	133	с	кириллическая строчная буква с
60	i	латинская строчная буква i	134	т	кириллическая строчная буква т
61	j	латинская строчная буква j	135	у	кириллическая строчная буква у
62	k	латинская строчная буква k	136	ф	кириллическая строчная буква ф
63	l	латинская строчная буква l	137	х	кириллическая строчная буква х
64	m	латинская строчная буква m	138	ц	кириллическая строчная буква ц
65	n	латинская строчная буква n	139	ч	кириллическая строчная буква ч
66	o	латинская строчная буква o	140	ш	кириллическая строчная буква ш
67	p	латинская строчная буква p	141	щ	кириллическая строчная буква щ
68	q	латинская строчная буква q	142	ъ	кириллическая строчная буква ъ
69	r	латинская строчная буква r	143	ы	кириллическая строчная буква ы
70	s	латинская строчная буква s	144	ь	кириллическая строчная буква ь
71	t	латинская строчная буква t	145	э	кириллическая строчная буква э
72	u	латинская строчная буква u	146	ю	кириллическая строчная буква ю
73	v	латинская строчная буква v	147	я	кириллическая строчная буква я

Приложение № 6

Форма доверенности пользователя удостоверяющего центра

Доверенность

_____ «_____» _____ 20___ г.

_____
_____
_____
наименование организации, включая организационно-правовую форму

в лице _____
(должность)

_____
(фамилия, имя, отчество)

действующего на основании _____

уполномочивает _____
(фамилия, имя, отчество)

_____
(серия и номер паспорта, кем и когда выдан)

1. Получить сертификат ключа проверки электронной подписи в Корпоративном удостоверяющем центре Госкорпорации «Росатом».
2. При использовании электронной подписи электронных документов, выступать в роли Пользователя Удостоверяющего центра и осуществлять действия в рамках Регламента Удостоверяющего центра по созданию и управлению квалифицированными сертификатами ключей проверки электронной подписи, установленные для Пользователя Удостоверяющего центра.

Настоящая доверенность действительна по «____» _____ 20____г.[1]

Подпись пользователя Удостоверяющего центра_____ _____,
фамилия, имя, отчество подпись

подтверждаю.

Уполномоченное должностное лицо
_____ _____ / _____ /
подпись Ф.И.О.

М.П.

[*] Примечание: срок действия доверенности должен быть не менее срока действия закрытого ключа, соответствующего создаваемому сертификату

Приложение № 7

Форма доверенности доверенного лица, наделённого правом получения ключевых носителей с ключами электронной подписи и сертификатов ключей проверки электронной подписи

Доверенность

_____ «_____» _____ 20___ г.

_____

_____

наименование организации, включая организационно-правовую форму

в лице _____

(должность)

_____

(фамилия, имя, отчество)

действующего на основании _____

уполномочивает _____

(фамилия, имя, отчество)

_____

(серия и номер паспорта, кем и когда выдан)

1. Предоставить в Корпоративный удостоверяющий центр Госкорпорации «Росатом» (КУЦ) необходимые документы, определённые Регламентом КУЦ, для сертификатов ключей проверки электронной подписи Пользователя(ей) КУЦ:

№ п.п.	Ф.И.О. Пользователя УЦ – владельца сертификата ключа проверки электронной подписи	Подпись
1.		

2. Получить созданные ключи и сертификаты ключа проверки электронной подписи на ключевых носителях и сертификаты ключей проверки электронной подписи на бумажных носителях для Пользователей КУЦ в вышеперечисленном списке.

Доверенное лицо наделяется правом подписи в соответствующих документах для исполнения поручений, определённых настоящей доверенностью.

Полномочия по настоящей доверенности не могут быть переданы другим лицам.

Настоящая доверенность действительна с момента выдачи по «___» _____ 20___ г.

Подпись доверенного лица _____ _____,

фамилия, имя, отчество подпись

подтверждаю.

Уполномоченное должностное лицо

_____ _____ / _____ /

подпись Ф.И.О.

Приложение № 8

Заявление на аннулирование сертификата ключа проверки электронной подписи

«_____» _____ 201__ г.

_____

_____

наименование организации, включая организационно-правовую форму

в лице _____,

должность

_____,

фамилия, имя, отчество

действующего на основании _____

Просит внести в реестр удостоверяющего центра информацию об аннулировании сертификата ключа проверки электронной подписи:

Серийный номер сертификата	
Причина аннулирования сертификата	

Владелец сертификата ключа проверки электронной подписи _____/_____/

(подпись) (ФИО)

Уполномоченное должностное лицо

_____ _____ / _____ /

(подпись) (ФИО)

«___»_____201__ г. М.П.

Отметки удостоверяющего центра

Отметка Оператора УЦ.
Данные, указанные в заявлении, проверены.
Сведения об аннулировании сертификата ключа проверки электронной подписи занесены в реестр УЦ

_____/_____/

«___»_____201__ г.

Приложение № 9

Заявление на приостановление действия сертификата ключа проверки электронной подписи

«_____» _____ 201__ г.

_____

_____

_____

наименование организации, включая организационно-правовую форму

в лице _____,

должность

_____,

фамилия, имя, отчество

действующего на основании _____

Просит внести в реестр удостоверяющего центра информацию о приостановлении действия сертификата ключа проверки электронной подписи:

Серийный номер сертификата	
Срок приостановления сертификата (минимальный срок 30 дней)	

Владелец сертификата ключа проверки электронной подписи _____/_____/

(подпись) (ФИО)

Уполномоченное должностное лицо

_____ _____ / _____ /

(подпись) (ФИО)

«___»_____201__ г. М.П.

Отметки удостоверяющего центра

Отметка Оператора УЦ.
Данные, указанные в заявлении, проверены.
Сведения о приостановлении действия сертификата ключа проверки электронной подписи занесены в реестр УЦ

_____/_____/

«___»_____201__ г.

Приложение № 10

Заявление на возобновление действия сертификата ключа проверки электронной подписи

«_____» _____ 201__ г.

_____

_____

_____

наименование организации, включая организационно-правовую форму

в лице _____,

должность

_____,

фамилия, имя, отчество

действующего на основании _____

Просит внести в реестр удостоверяющего центра информацию о возобновлении действия сертификата ключа проверки электронной подписи:

Серийный номер сертификата	

Владелец сертификата ключа проверки электронной подписи _____/_____/

(подпись) (ФИО)

Уполномоченное должностное лицо

_____ _____ / _____ /

(подпись) (ФИО)

«___»_____201__ г. М.П.

Отметки удостоверяющего центра

Отметка Оператора УЦ.
Данные, указанные в заявлении, проверены.
Сведения о возобновлении действия сертификата ключа проверки электронной подписи занесены в реестр УЦ

_____/_____/

«___»_____201__ г.

Приложение № 11

Заявление на подтверждение подлинности электронной подписи в электронном документе

«_____» _____ 201__ г.

_____

_____

_____

наименование организации, включая организационно-правовую форму

в лице _____,

должность

_____,

фамилия, имя, отчество

действующего на основании _____

Прошу подтвердить подлинность электронной подписи (ЭП) в электронном документе на основании следующих данных

1. Файл, содержащий сертификат ключа проверки электронной подписи, с использованием которого необходимо осуществить подтверждение подлинности ЭП в электронном документе на прилагаемом к заявлению носителе – рег. № _____;

2. Файл, содержащий подписанные ЭП данные и значение ЭП, либо файл, содержащий исходные данные и файл, содержащий значение ЭП, на прилагаемом к заявлению носителе – рег. № _____

3. Время, на момент наступления которого требуется подтвердить подлинность ЭП: _____

Способ получения заключения Удостоверяющего центра о подтверждении подлинности электронной подписи в электронном документе (отметить галочкой):

В Корпоративном удостоверяющем центре по адресу: г. Москва, 1-й Нагатинский проезд., д. 10, стр. 1, ком. 906	
Почтовым сообщением по адресу (указать адрес и имя получателя):	

Владелец сертификата ключа проверки электронной подписи _____/_____/

(подпись) (ФИО)

Уполномоченное должностное лицо

_____ _____ / _____ /

(подпись) (ФИО)

«___»_____201__ г. М.П.

Отметки удостоверяющего центра

Подготовлено заключение о подтверждении подлинности ЭП в электронном документе _____/_____/

«___»_____201__ г.

Заключение о подтверждении подлинности ЭП получено пользователем _____/_____/

«___»_____201__ г.

_____

Приложение № 12

Форма копии сертификата на бумажном носителе

Сведения о сертификате:
Кому выдан: CN
Кем выдан: Rosatom GOST CA
Действителен с <дата вступления в силу> по <дата окончания>
Версия: 3 (0x2)
Серийный номер: <Серийный номер>
Издатель сертификата: CN = Rosatom GOST CA, O = Госкорпорация "Росатом", L = Москва, S = г. Москва, C = RU, E = ca@rosatom.ru, Street = ул. Большая Ордынка д. 24, = 007706413348, = 1077799032926
Срок действия:
Действителен с: <дата вступления в силу>
Действителен по: <дата окончания>
Владелец сертификата: CN, OU, O, L, S, C, E, INN, SNILS, OGRN
Открытый ключ:
Алгоритм открытого ключа:
Название: <название алгоритма>
Идентификатор: <идентификатор алгоритма>
Значение: <значение открытого ключа>
Расширения сертификата X.509
1. Расширение 2.5.29.15 (критическое)
Название: Использование ключа
Значение: Цифровая подпись, Неотрекаемость, Шифрование ключей, Шифрование данных (f0)
2. Расширение 2.5.29.37
Название: Улучшенный ключ
Значение: Временный доступ к Центру Регистрации (1.2.643.2.2.34.2)
3. Расширение 2.5.29.14
Название: Идентификатор ключа субъекта
Значение: da 01 d1 46 47 58 69 b4 85 b3 1f cb 1e 22 cc 5f 9e 95 de 79
4. Расширение 2.5.29.35
Название: Идентификатор ключа центра сертификатов
Значение: Идентификатор ключа=46 e6 c6 29 7f 19 ed 18 05 94 b4 f4 4f 6c 00 cb b7 51 2c 2f Поставщик сертификата: <информация о поставщике сертификата>
5. Расширение 2.5.29.31
Название: Точки распространения списков отзыва (CRL)
Значение: [1]Точка распределения списка отзыва (CRL) Имя точки распространения: Полное имя: <перечень точек распространения СОС>
6. Расширение 1.3.6.1.5.5.7.1.1
Название: Доступ к информации о центрах сертификации
Значение: [1]Доступ к сведениям центра сертификации Метод доступа=Поставщик центра сертификации (1.3.6.1.5.5.7.48.2)
Дополнительное имя: <адрес размещения издающего сертификата>
7. Расширение 2.5.29.16
Название: Период использования закрытого ключа
Значение: Действителен с <дата вступления в силу> Действителен по <дата окончания>
8. Расширение 2.5.29.32
Название: Политики сертификата
Значение: [1]Политика сертификата: Идентификатор политики=1.2.643.100.113.1
9. Расширение 1.2.643.100.111
Значение: <Средство электронной подписи пользователя>
10. Расширение 1.2.643.100.112
Значение: <Средство электронной подписи издателя>
Подпись Удостоверяющего центра:
Алгоритм подписи:
Название: <название алгоритма>
Идентификатор: <идентификатор>
Значение: <значение открытого ключа издателя>

Подпись уполномоченного сотрудника УЦ: _____/_____
"___" _____ 201__ г.
М. П.

Подпись владельца сертификата: _____/_____
"___" _____ 201__ г.

Подписанную копию сертификата ключа проверки электронной подписи следует направить
в Корпоративный удостоверяющий центр ГК "Росатом" по адресу:
115230, 1-й Нагатинский проезд., д. 10, стр. 1

Приложение № 13

Формат сертификата ключа проверки электронной подписи

Название	Описание	Содержание
Базовые поля сертификата		
Version	Версия	V3
Serial Number	Серийный номер	Уникальный серийный номер сертификата
Signature Algorithm	Алгоритм подписи	ГОСТ Р 34.11/34.10-2001 **либо ГОСТ Р 34.11/34.10-2012**
Issuer	Издатель сертификата	1) commonName (общее имя). 4) countryName (наименование страны). 5) stateOrProvinceName (наименование штата или области). 6) localityName (наименование населенного пункта). 7) streetAddress (название улицы, номер дома). 8) organizationName (наименование организации). 9) organizationUnitName (подразделение организации). 10) title (должность). 11) OGRN (ОГРН). 12) INN (ИНН).
Validity Period	Срок действия сертификата	Действителен с (notBefore): дд.мм.гггг чч:мм:сс GMT Действителен по(notAfter): дд.мм.гггг чч:мм:сс GMT
Subject	Владелец сертификата	1) commonName (общее имя). 2) surname (фамилия). 3) givenName (приобретенное имя). 4) countryName (наименование страны). 5) stateOrProvinceName (наименование штата или области). 6) localityName (наименование населенного пункта). 7) streetAddress (название улицы, номер дома). 8) organizationName (наименование организации). 9) organizationUnitName (подразделение организации). 10) title (должность). 11) E = электронная почта 12) UnsructuredName (UN) 13) OGRN (ОГРН). 14) SNILS (СНИЛС). 15) INN (ИНН).
Public Key	Открытый ключ	Уникальный ключ проверки электронной подписи (алгоритм подписи)
Issuer Signature Algorithm	Алгоритм подписи издателя сертификата	ГОСТ Р 34.11/34.10-2001 **либо ГОСТ Р 34.11/34.10-2012**
Issuer Sign	ЭП издателя сертификата	Подпись издателя в соответствии с ГОСТ Р 34.11/34.10-2001 **либо ГОСТ Р 34.11/34.10-2012**
Расширения сертификата		
Private Key Validity Period	Срок действия закрытого ключа, соответствующего сертификату	Действителен с (notBefore): дд.мм.гггг чч:мм:сс GMT Действителен по(notAfter): дд.мм.гггг чч:мм:сс GMT
Key Usage	Использование ключа	Неотрекаемость - невозможность осуществления отказа от совершенных действий; Цифровая подпись, Шифрование ключей, Шифрование данных
Extended Key Usage	Улучшеный ключ	Могут быть внесены дополнительные области использования
Subject Key Idendifier	Идентификатор ключа владельца сертификата	Идентификатор закрытого ключа владельца сертификата
Authority Key Identifier	Идентификатор ключа издателя сертификата	Идентификатор закрытого ключа Уполномоченного лица удостоверяющего центра, на котором подписан данный сертификат
CRL Distribution Point	Точка распространения списка отозванных сертификатов	Набор адресов точек распространения списков отозванных сертификатов следующего вида:
certificatePolicies	Политики сертификата	Обозначение класса средств ЭП владельца квалифицированного сертификата
subjectSignTool		Наименование используемого владельцем квалифицированного сертификата средства ЭП
IssuerSignTool		Полное наименование средства ЭП, которое было использовано для создания ключа ЭП, ключа проверки ЭП и квалифицированного сертификата.
		Конкретный перечень используемых расширений устанавливается удостоверяющим центром
		В сертификат ключа подписи могут быть добавлены дополнительные поля и расширения согласно RFC 3280 и RFC 5280

Приложение № 14

Руководство по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи

Пользователь КУЦ обязан:

– соблюдать требования к обеспечению безопасности конфиденциальной информации с использованием средств квалифицированной электронной подписи;

– сдать средства квалифицированной электронной подписи и ключи электронной подписи, эксплуатационную и техническую документацию к ним в соответствии с порядком, установленным при увольнении или отстранении от исполнения обязанностей, связанных с использованием средств квалифицированной электронной подписи;

– немедленно уведомлять орган криптографической защиты о фактах утраты или недостачи средств квалифицированной электронной подписи, ключевых документов к ним, ключей от помещений, хранилищ, личных печатей и о других фактах, которые могут привести к разглашению защищаемых сведений конфиденциального характера, а также о причинах и условиях возможной утечки таких сведений

– обеспечивать конфиденциальность ключей электронной подписи, в частности не допускать использование принадлежащих ему ключей электронной подписи без его согласия;

– уведомлять КУЦ, выдавший сертификат ключа проверки электронной подписи, и иных участников электронного взаимодействия о нарушении конфиденциальности ключа электронной подписи в течение не более чем одного рабочего дня со дня получения информации о таком нарушении;

– использовать для создания и проверки квалифицированных электронных подписей, создания ключей квалифицированной электронной подписи и ключей их проверки средства электронной подписи, получившие подтверждение соответствия требованиям, установленным в соответствии с действующим Федеральным законодательством.

– не использовать ключ электронной подписи и немедленно обратиться в КУЦ для прекращения действия сертификата при наличии оснований полагать, что конфиденциальность ключа электронной подписи нарушена;

– использовать квалифицированную электронную подпись в соответствии с ограничениями, содержащимися в квалифицированном сертификате (если такие ограничения установлены).

– обновлять сертификат ключа проверки электронной подписи в соответствии с установленным регламентом.

– принять меры по исключению несанкционированного доступа в помещения, в которых размещены технические средства с установленным средством квалифицированной электронной подписи, посторонних лиц, по роду своей деятельности не являющихся персоналом, допущенным к работе в этих помещениях. В случае необходимости присутствия посторонних лиц в указанных помещениях должен быть обеспечен контроль за их действиями и обеспечена невозможность негативных действий с их стороны на средства квалифицированной электронной подписи, технические средства, на которых эксплуатируется средства квалифицированной электронной подписи и защищаемую информацию.

Пользователю КУЦ запрещается:

– оставлять без контроля вычислительные средства, на которых эксплуатируется средства квалифицированной электронной подписи, после ввода ключевой информации либо иной конфиденциальной информации;

– вносить какие-либо изменения в программное обеспечение средств квалифицированной электронной подписи;

– осуществлять несанкционированное администратором безопасности копирование ключевых носителей;

– разглашать содержимое носителей ключевой информации или передавать сами носители лицам, к ним не допущенным, выводить ключевую информацию на дисплей, принтер и т.п. иные средства отображения информации;

– использовать ключевые носители в режимах, не предусмотренных функционированием средств квалифицированной электронной подписи;

– записывать на ключевые носители постороннюю информацию;

– использовать нестандартные, изменённые или отладочные версии операционных систем (ОС).

– использовать ОС, отличную от предусмотренной штатной работой.

– использовать возможность удалённого управления, администрирования и модификации ОС и её настроек.

– разглашать содержимое носителей ключевой информации или передавать сами носители лицам, к ним не допущенным, выводить ключевую информацию на дисплей, принтер и т.п. иные средства отображения информации.

– использовать ключевые носители в режимах, не предусмотренных функционированием СКЗИ

– подключать к компьютеру с установленным средством квалифицированной электронной подписи дополнительные устройства и соединители, не предусмотренные штатной комплектацией.

– изменять настройки, установленные программой установки средства квалифицированной электронной подписи или администратором.

– обрабатывать на ПЭВМ, оснащённой средством квалифицированной электронной подписи, информацию, содержащую государственную тайну.

– осуществлять несанкционированное вскрытие системных блоков ПЭВМ.

Пользователь КУЦ несёт ответственность за:

– полноту и своевременность предоставления документов (в соответствии с Приложениями) в КУЦ;

– обеспечение конфиденциальности ключей ЭП, в частности не допущение использования принадлежащих ему ключей ЭП без его согласия;

– уведомление КУЦ, выдавшего сертификат ключа проверки ЭП, и иных участников электронного взаимодействия о нарушении конфиденциальности ключа ЭП в течение не более чем одного рабочего дня со дня получения информации о таком нарушении;

– не использование ключа ЭП при наличии оснований полагать, что конфиденциальность данного ключа нарушена.

Приложение № 15

Ограничения использования сертификатов ключей проверки электронной подписи

1. Квалифицированный сертификат Госкорпорации «Росатом»

Данные сертификаты ключа проверки электронной подписи предназначены для:

- аутентификации пользователей при доступе к корпоративным информационным системам ЦОД из сети Интернет;
- использования при участии в качестве заказчика на электронных торговых площадках;
- использования в защищённой корпоративной почтовой системе Госкорпорации «Росатом».

В сертификате указываются следующие ограничения:

В поле Дополнительное имя субъекта (UPN) = имя доменной учётной записи домена GK

В поле улучшенный ключ:

- Проверка подлинности клиента (1.3.6.1.5.5.7.3.2)
- Шифрующая файловая система (EFS) (1.3.6.1.4.1.311.10.3.4)
- Защищенная электронная почта (1.3.6.1.5.5.7.3.4)
- Вход со смарт-картой (1.3.6.1.4.1.311.20.2.2)
- Пользователь Центра Регистрации, HTTP, TLS клиент (1.2.643.2.2.34.6)

Срок действия сертификата - 1 год и 3 месяца.

Для обозначения класса средств ЭП владельца квалифицированного сертификата должны применяться следующий идентификатор:

- 1.2.643.100.113.1 - класс средства ЭП КС 1

2. Квалифицированная подпись в ЕОСДО

Данные сертификаты ключа проверки электронной подписи предназначены для подписи электронных документов в Единой отраслевой системе документооборота ГК «Росатом».

В поле Дополнительное имя субъекта:

UPN = имя доменной учётной записи домена GK

В сертификате указываются следующие ограничения:

- Подпись документов в ЕОСДО (1.2.643.3.168.1.1)
- Пользователь Центра Регистрации, HTTP, TLS клиент (1.2.643.2.2.34.6)
- Проверка подлинности клиента (1.3.6.1.5.5.7.3.2)

Срок действия сертификата - 1 год и 3 месяца.

Для обозначения класса средств ЭП владельца квалифицированного сертификата должны применяться следующий идентификатор:

- 1.2.643.100.113.1 - класс средства ЭП КС 1

3. Аутентификация сервера

Данные сертификаты ключа проверки электронной подписи предназначены для применения в следующих автоматизированных системах:

- Аутентификация сервера.

В сертификате указываются следующие дополнительные поля:

В поле улучшенный ключ:

- Проверка подлинности сервера (1.3.6.1.5.5.7.3.1)

Срок действия сертификата - 1 год и 3 месяца.

Для обозначения класса средств ЭП владельца квалифицированного сертификата должны применяться следующий идентификатор:

- 1.2.643.100.113.1 - класс средства ЭП КС 1

4. Клиент S-Terra (КСПД)

Данные сертификаты предназначены для применения в АРМ Корпоративной сети передачи данных.

Создание данных сертификатов осуществляется при совместном формировании дистрибутива Клиента КСПД в Органе криптографической защиты АО «Гринатом»

В поле Дополнительное имя субъекта:

UPN = имя доменной учётной записи домена GK

В сертификате указываются следующие дополнительные поля:

В поле улучшенный ключ:

- Проверка подлинности клиента (1.3.6.1.5.5.7.3.2)
- Пользователь Центра Регистрации, HTTP, TLS клиент (1.2.643.2.2.34.6)

Срок действия сертификата - 1 год и 3 месяца.

Для обозначения класса средств ЭП владельца квалифицированного сертификата должны применяться следующий идентификатор:

- 1.2.643.100.113.1 - класс средства ЭП КС 1

5. Шлюз КСПД

Данные сертификаты ключа проверки электронной подписи предназначены для применения в следующих автоматизированных системах:

- Узел Корпоративной системы передачи данных;

В сертификате указываются следующие дополнительные поля:

В поле улучшенный ключ:

- Проверка подлинности сервера (1.3.6.1.5.5.7.3.1)

Срок действия сертификата - 1 год и 3 месяца.

Для обозначения класса средств ЭП владельца квалифицированного сертификата должны применяться следующий идентификатор:

- 1.2.643.100.113.1 - класс средства ЭП КС 1
- 1.2.643.100.113.2 - класс средства ЭП КС 2

6. СЦУД

Данные сертификаты ключа проверки электронной подписи предназначены для использования в системе централизованного управления доступом Госкорпорации «Росатом».

В сертификате указываются следующие ограничения:

В поле Дополнительное имя субъекта:

UPN = имя доменной учётной записи домена GK

В поле улучшенный ключ:

- Проверка подлинности клиента (1.3.6.1.5.5.7.3.2)
- Согласование заявок на предоставление ресурсов в СЦУД (1.2.643.3.168.1.2)
- Пользователь Центра Регистрации, HTTP, TLS клиент (1.2.643.2.2.34.6)

Срок действия сертификата - 1 год и 3 месяца.

Для обозначения класса средств ЭП владельца квалифицированного сертификата должны применяться следующий идентификатор:

- 1.2.643.100.113.1 - класс средства ЭП КС 1

7. Квалифицированный сертификат Госкорпорации «Росатом» + Росреестр

(для получения требуется дополнительно предоставить документ, подтверждающий право лица действовать от имени юридического лица без доверенности, или, в случае получения электронной подписи лицом, получившим доверенность от правообладателя, доверенность, подписанная руководителем организации или иным лицом, уполномоченным на это учредительными документами юридического лица, заверенная печатью этой организации)

Данные сертификаты ключа проверки электронной подписи предназначены для:

- аутентификации пользователей при доступе к корпоративным информационным системам ЦОД из сети Интернет;
- использования при участии в качестве заказчика на электронных торговых площадках;

- использования в защищённой корпоративной почтовой системе Госкорпорации «Росатом»;
- Выписка из Единого государственного реестра юридических лиц

В сертификате указываются следующие ограничения:

В поле Дополнительное имя субъекта (UPN) = имя доменной учётной записи домена GK

В поле улучшенный ключ:

- Проверка подлинности клиента (1.3.6.1.5.5.7.3.2)
- Шифрующая файловая система (EFS) (1.3.6.1.4.1.311.10.3.4)
- Защищенная электронная почта (1.3.6.1.5.5.7.3.4)
- Вход со смарт-картой (1.3.6.1.4.1.311.20.2.2)
- Пользователь Центра Регистрации, HTTP, TLS клиент (1.2.643.2.2.34.6)
- Формирование запроса о предоставлении сведений из Единого государственного реестра прав на недвижимое имущество и сделок с ним и о предоставлении сведений из государственного кадастра недвижимости (1.2.643.5.1.24.2.30)

Срок действия сертификата - 1 год и 3 месяца.

Для обозначения класса средств ЭП владельца квалифицированного сертификата должны применяться следующий идентификатор:

- 1.2.643.100.113.1 - класс средства ЭП КС 1

8. Тестовый сертификат

Данные сертификаты ключа проверки электронной подписи предназначены для тестирования возможности применения электронной подписи в автоматизированных/информационных системах:

В сертификате указываются следующие дополнительные поля:

- Временный доступ к центру регистрации (1.2.643.2.2.34.2)

По согласованию с Удостоверяющим центром в сертификат могут быть внесены дополнительные ограничения.

Срок действия сертификата - 2 месяца.

Для обозначения класса средств ЭП владельца квалифицированного сертификата должны применяться следующий идентификатор:

- 1.2.643.100.113.1 - класс средства ЭП КС 1

9. Облачная подпись Госкорпорации «Росатом»

Данные сертификаты ключа проверки электронной подписи предназначены для Формирования квалифицированной электронной в Системе электронной подписи Госкорпорации «Росатом». В качестве ключевого контейнера используется Система электронной подписи Госкорпорации «Росатом»

В сертификате указываются следующие ограничения:

В поле Дополнительное имя субъекта (UPN) = имя доменной учётной записи домена GK

В поле улучшенный ключ:

- Проверка подлинности клиента (1.3.6.1.5.5.7.3.2)
- Защищенная электронная почта (1.3.6.1.5.5.7.3.4)
- Пользователь Центра Регистрации, HTTP, TLS клиент (1.2.643.2.2.34.6)

Срок действия сертификата - 1 год и 3 месяца.

Для обозначения класса средств ЭП владельца квалифицированного сертификата должны применяться следующий идентификатор:

- 1.2.643.100.113.1 - класс средства ЭП КС 1

10. Неквалифицированный сертификат Госкорпорации «Росатом»

Данные сертификаты ключа проверки электронной подписи выпускаются самоподписанным сертификатом Центра сертификации «Росатом» и предназначены для:

- использования в во всех отраслевых системах, где законодательно не требуется квалифицированная подпись
- аутентификации пользователей при доступе к корпоративным информационным системам ЦОД из сети Интернет;
- использования в защищённой корпоративной почтовой системе Госкорпорации «Росатом»;

В сертификате указываются следующие ограничения:

В поле Дополнительное имя субъекта (UPN) = имя доменной учётной записи домена GK

В поле улучшенный ключ:

- Проверка подлинности клиента (1.3.6.1.5.5.7.3.2)
- Шифрующая файловая система (EFS) (1.3.6.1.4.1.311.10.3.4)
- Защищенная электронная почта (1.3.6.1.5.5.7.3.4)
- Вход со смарт-картой (1.3.6.1.4.1.311.20.2.2)
- Пользователь Центра Регистрации, HTTP, TLS клиент (1.2.643.2.2.34.6)
- Формирование запроса о предоставлении сведений из Единого государственного реестра прав на недвижимое имущество и сделок с ним и о предоставлении сведений из государственного кадастра недвижимости (1.2.643.5.1.24.2.30)

Срок действия сертификата - 1 год и 3 месяца.

Для обозначения класса средств ЭП владельца квалифицированного сертификата должны применяться следующий идентификатор:

- 1.2.643.100.113.1 - класс средства ЭП КС 1

Приложение № 16

Перечень областей использования сертификатов, зарегистрированных в КУЦ

В Российском пространстве телекоммуникационных объектных идентификаторов за УЦ ГК «Росатом» зарегистрировано уникальное значение в соответствии с ISO 8824-1 |ITU-T X.680, ISO3166 , ГОСТ Р ИСО/МЭК 8824-1-2003. В качестве корневого объектного идентификатора для построения структуры идентификаторов областей применения сертификатов открытых ключей Удостоверяющим Центром используется значение 1.2.643.3.168

Структура объектных идентификаторов областей применения сертификатов ключа проверки электронной подписи Удостоверяющего имеет вид:

№	Корневой OID	Область применения	OID	Значение
1.	1.2.643.3.168.1.	Автоматизированные системы	1.2.643.3.168.1.1	ЕОСДО
			1.2.643.3.168.1.2	Согласование заявок на предоставление ресурсов в СЦУД
2.	1.2.643.3.168.2.	Системные роли	1.2.643.3.168.2.1	Администратор ключевой документации СКЗИ узлов КСПД (Администратор КД)
3.	1.2.643.3.168.3.	Политики выдачи		
4.	1.2.643.3.168.4.	Политики применения	1.2.643.3.168.4.1	Тестирование системы подписания проектно-сметной документации.
5.	1.2.643.3.168.5.	Политики штампов времени	1.2.643.3.168.5.1	Политика штампов времени по-умолчанию

В случае необходимости, для увеличения уровня детализации областей применения сертификатов открытых ключей, возможно введение дополнительного деления объектных идентификаторов.

Приложение № 2 к Дополнительному соглашению № 22/2143-Д-10 от 01 мая 2018 г.
к Договору присоединения №22/2143-Д от 06 июля 2012 г.
(Приложение № 6 к Договору присоединения № 22/2143-Д от 06 июля 2012 г.)

У Т В Е Р Ж Д А Ю

Заместитель директора по информационным технологиям

_____ / С.Н. Данилов
(подпись) (Ф.И.О)

М.П. (по доверенности № 22/56/2018-ДОВ от 26.04.2018)

Регламент процесса «Контроль (оценка) уровня доверия и контроль приведения в соответствие требованиям Госкорпорации «Росатом» защищенных с использованием шифровальных (криптографических) средств информационных и телекоммуникационных систем»

Редакция №1

2018

Оглавление

1. Назначение и область применения

Настоящий регламент процесса «Контроль (оценка) уровня доверия и контроль приведения в соответствие требованиям Госкорпорации «Росатом» защищенных с использованием шифровальных (криптографических) средств информационных и телекоммуникационных систем» (далее – Регламент), разработан в соответствии с действующим законодательством Российской Федерации, регламентирующим деятельность органов криптографической защиты (далее – ОКЗ).

Настоящий Регламент определяет условия предоставления и правила пользования услугой ОКЗ по контролю (оценке) уровня доверия и контролю приведения в соответствие требованиям Госкорпорации «Росатом» защищенных с использованием шифровальных (криптографических) средств информационных и телекоммуникационных систем, основные организационно-технические мероприятия, направленные на обеспечение работы ОКЗ. Регламент имеет статус локального.

Требования настоящего Регламента распространяются на организации-обладатели конфиденциальной информации (далее - ООКИ), использующие защищенные с использованием шифровальных (криптографических) средств информационные и телекоммуникационные системы и обязательны для выполнения сотрудниками, исполняющими следующие функциональные роли:

1. Руководитель ООКИ;
2. Руководитель Органа криптографической защиты АО «Гринатом»;
3. Проверяющий.

Настоящий Регламент использует ссылки на следующие документы, необходимые для управления процессом «Контроль (оценка) уровня доверия и контроль приведения в соответствие требованиям Госкорпорации «Росатом» защищенных с использованием шифровальных (криптографических) средств информационных и телекоммуникационных систем»:

Документ	Статус	Тип документа	Ответственный
Лицензия ФСБ России ЛСЗ №0014254 Рег.№15686Н от 19.01.2017 на осуществление разработки, производства, распространения шифровальных (криптографических) средств, информационных и телекоммуникационных систем, защищённых с использованием шифровальных (криптографических) средств, выполнения работ, оказания услуг в области шифрования информации, технического обслуживания шифровальных (криптографических) средств, информационных	Действует	Лицензия	Начальник управления информационной безопасности АО «Гринатом»

и телекоммуникационных систем, защищённых с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных и телекоммуникационных систем, защищённых с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)			
Федеральный закон Российской Федерации от 06.04.11 г. № 63-ФЗ "Об электронной подписи"	Действует	Федеральный закон	Начальник управления информационной безопасности АО «Гринатом»
Приказ ФАПСИ № 152 от 13.06.2001 г. «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну»	Действует	Приказ	Начальник управления информационной безопасности АО «Гринатом»
Приказ ФСБ № 66 от 09.02.2005 г. «Об утверждении положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)»	Действует	Приказ	Начальник управления информационной безопасности АО «Гринатом»
Отраслевые требования по информационной безопасности Госкорпорации «Росатом» №1/910-П-дсп от 23.09.2014	Действует	Требование	Начальник управления информационной безопасности АО «Гринатом»
Единые отраслевые методические указания по дистанционному банковскому обслуживанию в Госкорпорации «Росатом» и ее организациях, утв. Приказом от 22.10.2015 №1/1009-П (далее – ЕОМУ)	Действует	Указания	Руководители организаций ГК «Росатом»

и является основой для регламентации следующих подпроцессов и процедур:

Подпроцессы:
Подпроцесс «Контроль (оценка) уровня доверия к Системе»

2. Термины, определения и сокращения

Термин	Определение
Владелец Системы	Организация, предоставляющая на договорной основе организации обладателю конфиденциальной информации в пользование информационную/ телекоммуникационную систему, защищенную с использованием шифровальных (криптографических) средств
Ключевая информация	Специальным образом организованная совокупность криптоключей, предназначенная для осуществления криптографической защиты информации в течение определенного срока
Конфиденциальная информация	Информация с ограниченным доступом, не содержащая сведений, составляющих государственную тайну
Обладатели конфиденциальной информации	Государственные органы, государственные организации и другие организации независимо от их организационно-правовой формы и формы собственности, индивидуальные предприниматели и физические лица
Орган криптографической защиты	Действующая на постоянной основе рабочая группа из числа сотрудников Управления информационной безопасности
Пользователи СКЗИ	Физические лица, непосредственно допущенные к работе с СКЗИ
Система	Информационная/телекоммуникационная система, защищенная с использованием шифровальных (криптографических) средств
Средства криптографической защиты информации	Средства шифрования - аппаратные, программные и программно-аппаратные шифровальные (криптографические) средства, реализующие алгоритмы криптографического преобразования информации для ограничения доступа к ней, в том числе при ее хранении, обработке и передаче; средства имитозащиты - аппаратные, программные и программно-аппаратные шифровальные (криптографические) средства (за исключением средств шифрования), реализующие алгоритмы криптографического преобразования информации для ее защиты от навязывания ложной информации, в том числе защиты от модифицирования, для обеспечения ее достоверности и некорректируемости, а также обеспечения возможности выявления изменений, имитации, фальсификации или модифицирования информации;

	средства электронной подписи; средства кодирования - средства шифрования, в которых часть криптографических преобразований информации осуществляется с использованием ручных операций или с использованием автоматизированных средств, предназначенных для выполнения таких операций; средства изготовления ключевых документов - аппаратные, программные, программно-аппаратные шифровальные (криптографические) средства, обеспечивающие возможность изготовления ключевых документов для шифровальных (криптографических) средств, не входящие в состав этих шифровальных (криптографических) средств; ключевые документы - электронные документы на любых носителях информации, а также документы на бумажных носителях, содержащие ключевую информацию ограниченного доступа для криптографического преобразования информации с использованием алгоритмов криптографического преобразования информации (криптографический ключ) в шифровальных (криптографических) средствах; аппаратные шифровальные (криптографические) средства - устройства и их компоненты, в том числе содержащие ключевую информацию, обеспечивающие возможность преобразования информации в соответствии с алгоритмами криптографического преобразования информации без использования программ для электронных вычислительных машин; программные шифровальные (криптографические) средства - программы для электронных вычислительных машин и их части, в том числе содержащие ключевую информацию, обеспечивающие возможность преобразования информации в соответствии с алгоритмами криптографического преобразования информации в программно-аппаратных шифровальных (криптографических) средствах, информационных системах и телекоммуникационных системах, защищенных с использованием шифровальных (криптографических) средств;

	программно-аппаратные шифровальные (криптографические) средства - устройства и их компоненты (за исключением информационных систем и телекоммуникационных систем), в том числе содержащие ключевую информацию, обеспечивающие возможность преобразования информации в соответствии с алгоритмами криптографического преобразования информации с использованием программ для электронных вычислительных машин, предназначенных для осуществления этих преобразований информации или их части.
Электронная подпись	Информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию

Сокращение	Расшифровка
ОКЗ	Орган криптографической защиты АО «Гринатом»
ООКИ	Организация-обладатель конфиденциальной информации
СЗИ от НСД	Средство защиты информации от несанкционированного доступа
СКЗИ	Средства криптографической защиты информации

3. Описание процесса

3.1. Цель процесса

Предоставление услуг ОКЗ по контролю (оценке) уровня доверия и контролю приведения в соответствие требованиям Госкорпорации «Росатом» защищенных с использованием шифровальных (криптографических) средств информационных и телекоммуникационных систем.

3.2. Задачи процесса

- Контроль (оценка) уровня доверия к Системе;
- Контроль приведения в соответствие и мониторинг актуальности Системы.

3.3. Участники группы процессов и их роли

№ п.п.	Участники	Основные роли

1	Руководитель ООКИ	• Принимает решение о необходимости/об отказе от контроля (оценки) уровня доверия и контроля приведения в соответствие требованиям Госкорпорации «Росатом» защищенных с использованием шифровальных (криптографических) средств информационных и телекоммуникационных систем; • Согласовывает документы, необходимые для получения/отказа от услуг ОКЗ по контролю (оценке) уровня доверия и контролю приведения в соответствие требованиям Госкорпорации «Росатом» защищенных с использованием шифровальных (криптографических) средств информационных и телекоммуникационных систем.
2	Руководитель ОКЗ	• Принимает решение об оказании услуги ООКИ/об отказе от оказания услуги ООКИ по контролю (оценке) уровня доверия и контролю приведения в соответствие требованиям Госкорпорации «Росатом» защищенных с использованием шифровальных (криптографических) средств информационных и телекоммуникационных систем; • Согласовывает документы необходимые для оказания услуги/отказа от оказания услуги по контролю (оценке) уровня доверия и контролю приведения в соответствие требованиям Госкорпорации «Росатом» защищенных с использованием шифровальных (криптографических) средств информационных и телекоммуникационных систем.
3	Проверяющий	• Формирует письма Владельцу Системы на предоставление документов по Системе; • Проводит анализ полученных от Владельца Системы документов; • Формирует и направляет в ООКИ Заключение по результатам оценки уровня доверия Системе (далее – Заключение ОКЗ); • Проводит мониторинг актуальности уровня доверия к Системе; • Формирует и направляет Владельцу Системы письма на приведение Системы в соответствие с ЕОМУ; • Проводит анализ документов, полученных от Владельца Системы, по приведению Системы в соответствие с ЕОМУ; • Формирует и направляет в ООКИ отчеты (по запросу ООКИ) о реализации рекомендаций по результатам оценки уровня доверия к Системе за период (далее – Отчет о проведенных работах).

3.4. Основные выходы процесса

№ п/п	Наименование основного выхода процесса (результата)	Потребитель основного выхода (клиент)	
		Группа процессов/ внешний контрагент	Уровень управления (Корпорация,/ Дивизион/ Организация)
1	2	3	4
1	Заявление на осуществление контроля (оценки) уровня доверия и контроля приведения в соответствие требованиям Госкорпорации «Росатом» защищенных с использованием шифровальных (криптографических) средств информационных и телекоммуникационных систем	АО «Гринатом»	Организация
2	Скан-копии заключенных/проекты заключаемых договоров (доп. соглашений) на Систему	АО «Гринатом»	Организация
3	Скан-копии документов по аттестации на соответствие требованиям безопасности объекта информатизации, где обрабатывается конфиденциальная информация	АО «Гринатом»	Организация
4	Письмо в ООКИ об отказе от контроля (оценки) уровня доверия и контроля приведения в соответствие требованиям Госкорпорации «Росатом» защищенных с использованием шифровальных (криптографических) средств информационных и телекоммуникационных систем	АО «Гринатом»	Организация
5	Письмо Владельцу Системы с запросом о предоставлении документов по Системе	Владелец Системы	Организация
6	Заключение ОКЗ	Предприятие	Организация
7	Письмо Владельцу Системы с рекомендациями по устранению выявленных недостатков	Владелец Системы	Организация
8	Отчет о проведенных работах (по запросу ООКИ)	Предприятие	Организация

3.5. Основные входы процесса

№ п/п	Наименование основного входа	Поставщик основного входа

	процесса	Группа процессов/ внешний контрагент	Уровень управления (Корпорация/ Дивизион/ Организация).
1	Единые отраслевые методические указания по дистанционному банковскому обслуживанию в Госкорпорации«Росатом» и ее организациях, утв. Приказом от 22.10.2015 №1/1009-П	ГК «Росатом»	Корпорация
2	Скан-копии заключенных/проекты заключаемых договоров (доп. соглашений) на Систему	Предприятие	Корпорация
3	Скан-копии документов по аттестации на соответствие требованиям безопасности объекта информатизации, где обрабатывается конфиденциальная информация	Предприятие	Организация
4	Документы от Владельца Системы	Владелец Системы	Организация
5	Заключение ОКЗ	АО «Гринатом»	Организация
6	Письмо от Владельца Системы по устранению недостатков/планом устранения недостатков	Владелец Системы	Организация
7	Отчет о проведенных работах (по запросу ООКИ)	АО «Гринатом»	Организация

3.6. Описание подпроцессов

3.6.1. Подпроцесс «Контроль (оценка) уровня доверия к Системе»

Руководитель ООКИ:

- Принимает решение о необходимости/об отказе от контроля (оценки) уровня доверия и контроля приведения в соответствие требованиям Госкорпорации «Росатом» защищенных с использованием шифровальных (криптографических) средств информационных и телекоммуникационных систем.

В случае если принимается решение о необходимости контроля (оценки) уровня доверия и контроля приведения в соответствие требованиям Госкорпорации «Росатом» защищенных с использованием шифровальных (криптографических) средств информационных и телекоммуникационных систем, согласно ЕОМУ:

- Направляет в ОКЗ следующий комплект документов:

– Оригинал подписанного Заявления на осуществление контроля (оценки) уровня доверия и контроля приведения в соответствие требованиям Госкорпорации «Росатом» защищенных с использованием шифровальных

(криптографических) средств информационных и телекоммуникационных систем (Приложение №4);

– Скан-копии заключенных/проекты заключаемых договоров (дополнительных соглашений) на Систему;

– Скан-копии документов по аттестации на соответствие требованиям безопасности объекта информатизации, где обрабатывается конфиденциальная информация.

В случае если принимается решение об отказе от контроля (оценки) уровня доверия и контроля приведения в соответствие требованиям Госкорпорации «Росатом» защищенных с использованием шифровальных (криптографических) средств информационных и телекоммуникационных систем:

- Направляет в ОКЗ письмо свободного формата об отказе от контроля (оценки) уровня доверия и контроля приведения в соответствие требованиям Госкорпорации «Росатом» защищенных с использованием шифровальных (криптографических) средств информационных и телекоммуникационных систем.

Руководитель ОКЗ:

- Принимает решение об оказании услуги/об отказе от оказания услуги на основании полученных документов.

Проверяющий:

В случае если принимается решение об оказании услуги:

- Направляет Владельцу Системы письмо с запросом о предоставлении документов по Системе согласно ЕОМУ (письмо может направляться от лица ООКИ, в этом случае проверяющий направляет в ООКИ проект письма с запросом о предоставлении документов по Системе):
- Проводит первичный/повторный анализ документов, присланных ООКИ и Владельцем Системы;
- Формирует Заключение ОКЗ (Приложение №5);
- Направляет Заключение ОКЗ в ООКИ.

Исходящая информация поступает в подпроцесс «Контроль приведения в соответствие и мониторинг актуальности Системы».

В случае если принимается решение об отказе в оказании услуги:

- Подготавливает и направляет в ООКИ письмо свободного формата об отказе от предоставления услуги по контролю (оценке) уровня доверия и контролю приведения в соответствие требованиям Госкорпорации «Росатом»

защищенных с использованием шифровальных (криптографических) средств информационных и телекоммуникационных систем.

Взаимодействие ООКИ и ОКЗ завершается.

3.6.2. Подпроцесс «Контроль приведения в соответствие и мониторинг актуальности Системы»

Входящая информация поступает из подпроцесса «Контроль (оценка) уровня доверия к Системе».

Проверяющий:

3.6.2.1. В случае если Система соответствует ЕОМУ:

- Проводит постоянный мониторинг актуальности уровня доверия в соответствии с информацией, изложенной в Заключении ОКЗ. Осуществляет мониторинг сроков действия всех документов, которые имеют отношение к Системе и влияют на уровень доверия;
- Формирует отчет о проведенных работах (по запросу ООКИ) (Приложение №6);
- Направляет Отчет о проведенных работах в ООКИ (по запросу ООКИ).

3.6.2.1.1. В случае если уровень доверия к Системе изменился:

Информация поступает в подпроцесс «Контроль (оценка) уровня доверия к Системе» на этап отправки Владельцу Системы письма с запросом о предоставлении документов по Системе согласно ЕОМУ.

3.6.2.1.2. В случае если уровень доверия к Системе не изменился:

- Проводит постоянный мониторинг актуальности уровня доверия в соответствии с информацией, изложенной в Заключении ОКЗ. Осуществляет мониторинг сроков действия всех документов, которые имеют отношение к Системе и влияют на уровень доверия (в соответствии с п. 3.6.2.1).

3.6.2.2. В случае если Система не соответствует ЕОМУ:

- Формирует в соответствии с Заключением ОКЗ письмо Владельцу Системы с рекомендациями по устранению выявленных недостатков и приведению Системы в соответствие с ЕОМУ (далее – письмо с рекомендациями. Письмо формируется от имени ООКИ или от имени ОКЗ в зависимости от договоренности с Владельцем Системы и с ООКИ). К письму могут прилагаться типовые схемы подключения (Приложение №7);
- Направляет письмо с рекомендациями Владельцу Системы (либо в ООКИ для последующей отправки Владельцу Системы);

- Проводит анализ информации, полученной от Владельца Системы в ответ на письмо с рекомендациями;
- Формирует Отчет о проведенных работах (по запросу ООКИ);
- Направляет Отчет о проведенных работах в ООКИ (по запросу ООКИ).

3.6.2.2.1. Если уровень доверия к Системе изменился:

Информация поступает в подпроцесс «Контроль (оценка) уровня доверия к Системе» на этап отправки Владельцу Системы письма с запросом о предоставлении документов по Системе согласно ЕОМУ.

3.6.2.2.2. Если уровень доверия не изменился:

- Проводит работы в соответствии с п. 3.6.2.1 или 3.6.2.2.

4. Нормативные ссылки

– Федеральный закон от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации»;
– Приказ ФАПСИ № 152 от 13.06.2001г. «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну»;
– Приказ ФСБ № 66 от 09.02.2005г «Об утверждении положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)»;
– Федеральный закон Российской Федерации от 06.04.11 г. № 63-ФЗ "Об электронной подписи";
– Федеральный закон от 04.05.2011 N 99-ФЗ "О лицензировании отдельных видов деятельности";
– Лицензия ФСБ России ЛСЗ №0014254 Рег.№15686Н от 19.01.2017 на осуществление разработки, производства, распространения шифровальных (криптографических) средств, информационных и телекоммуникационных систем, защищённых с использованием шифровальных (криптографических) средств, выполнения работ, оказания услуг в области шифрования информации, технического обслуживания шифровальных (криптографических) средств, информационных и телекоммуникационных систем, защищённых с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных и телекоммуникационных систем, защищённых с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя);
– Отраслевые требования по информационной безопасности Госкорпорации «Росатом» безопасности №1/910-П-дсп от 23.09.2014;

– Постановление №313 от 16.04.2012 г. Об утверждении Положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя);
– Единые отраслевые методические указания по дистанционному банковскому обслуживанию в Госкорпорации «Росатом» и ее организациях, утв. Приказом от 22.10.2015 №1/1009-П.

5. Порядок внесения изменений

Внесение изменений (дополнений) в Регламент, а также в приложения к нему, производится посредством утверждения новой редакции Регламента.

6. Контроль и ответственность

6.1. Регламент обязаны соблюдать все следующие участники процесса:

Руководитель ООКИ;
Руководитель ОКЗ;
Проверяющий.

6.2. Ответственность работников за несоблюдение требований Регламента

За несоблюдение Регламента ответственные лица несут административную и дисциплинарную ответственность в соответствии с действующим законодательством.

7. Перечень приложений

Приложение №1.	Матрица ответственности.
Приложение №2.	Схема процесса.
Приложение №3.	Дополнительные выходы и дополнительные входы.
Приложение №4.	Шаблон Заявления на осуществление контроля (оценки) уровня доверия и контроля приведения в соответствие требованиям Госкорпорации «Росатом» защищенных с использованием шифровальных (криптографических) средств информационных и телекоммуникационных систем.
Приложение №5.	Шаблон Заключения ОКЗ.
Приложение №6.	Шаблон Отчета о проведенных работах.

Приложение №7. Типовые схемы подключения.

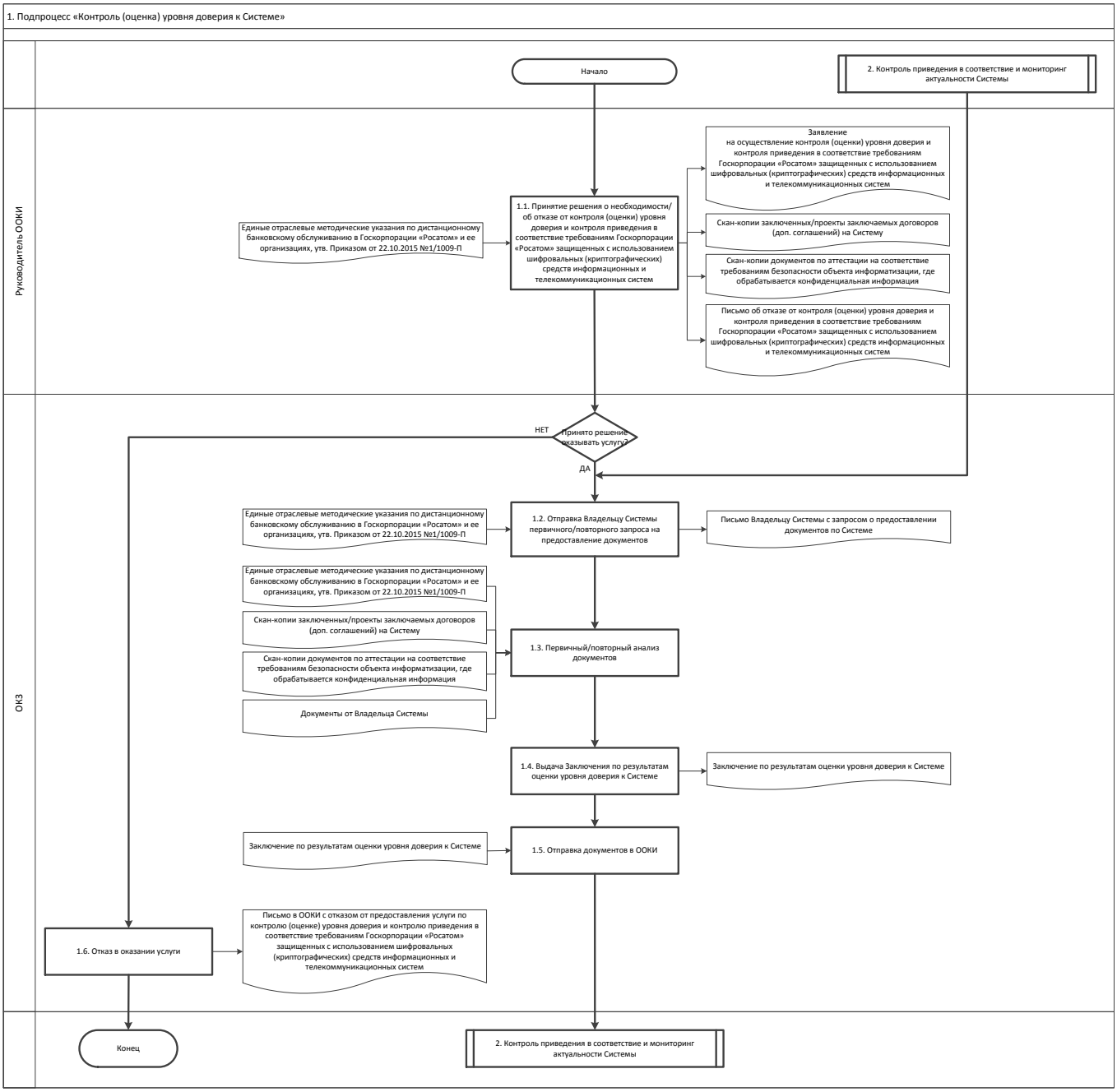
Приложение №1. Матрица ответственности

Подпроцессы в составе процесса	Участники процесса		
	Руководитель ООКИ	Руководитель ОКЗ	Проверяющий
Подпроцесс «Контроль (оценка) уровня доверия к Системе»	Утв	Утв	О
Подпроцесс «Контроль приведения в соответствие и мониторинг актуальности Системы»	Инф	Утв	О

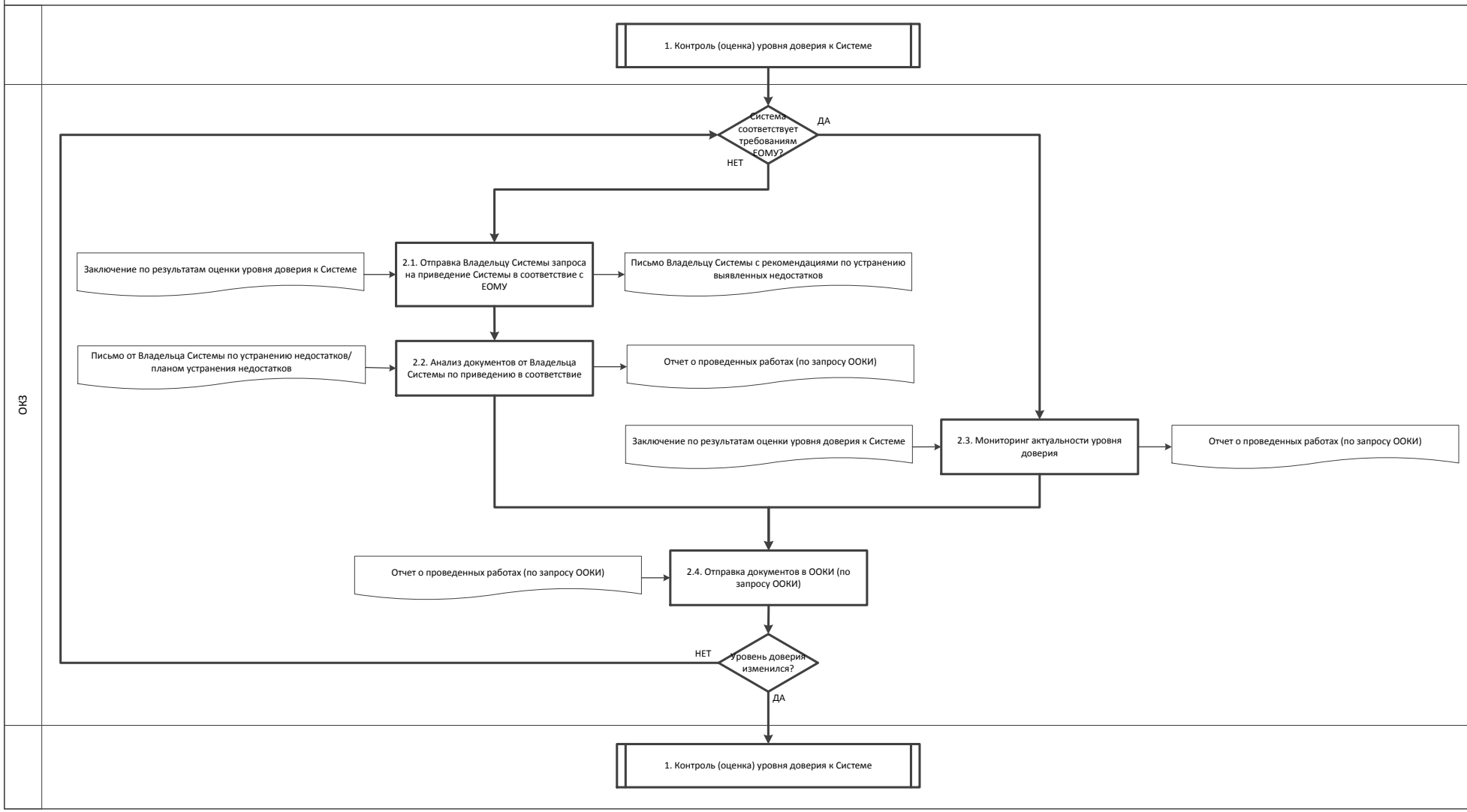
Сокращение	Название роли	Определение	Исполнитель Роли
М	Методолог	Формирует требования к организации деятельности в рамках подпроцесса/процедуры	Структурное подразделение Корпорации/Дивизиона/ Организации
И	Интегратор	Интегрирует результаты подпроцесса/процедуры и отвечает за организацию подпроцесса/процедуры, включая взаимодействие участников	Структурное подразделение Корпорации/Дивизиона/ Организации
К	Контролер	Осуществляет контроль выполнения и достижения результатов подпроцесса/процедуры	Структурное подразделение Корпорации/Дивизиона/ Организации Руководитель Корпорации/Дивизиона/ Организации
О	Ответственный	Несет ответственность за достижение результата по подпроцессу/процедуре в своей предметной области	Структурное подразделение Корпорации/Дивизиона/ Организации Руководитель Корпорации/Дивизиона/ Организации
Утв	Утверждающий	Утверждает - принимает окончательное решение по результату подпроцессу/процедуре	Коллегиальные органы (Наблюдательный совет, Правление и прочие) Генеральный директор Корпорации, Руководители Корпорации /Дивизионов/Организаций

С	Согласовывающий	Согласовывает /одобряет результаты подпроцесса/процедуры для дальнейшего принятия решений	Коллегиальные органы Руководители Корпорации/ Дивизионов/ Организаций
Э	Экспертирующий	Осуществляет экспертизу по подпроцессу/процедуре	Коллегиальные органы Структурное подразделение Корпорации/Дивизиона/ Организации
Инф	Информируемый	Получает информацию о ходе/результате подпроцесса /процедуры	Структурное подразделение Корпорации/Дивизиона/ Организации Руководитель Корпорации/Дивизиона/ Организации Коллегиальные органы

Приложение №2. Схема процесса



2. Подпроцесс «Контроль приведения в соответствие и мониторинг актуальности Системы»



Приложение №3. Дополнительные выходы и дополнительные входы

№ п/п	Наименование дополнительного выхода процесса	Потребитель дополнительного выхода процесса (группа процессов/ внешний контрагент)

№ п/п	Наименование дополнительного входа процесса	Поставщик дополнительного входа процесса (группа процессов/ внешний контрагент)

Приложение №4. Шаблон Заявления на контроль (оценку) уровня доверия и контроль приведения в соответствие требованиям Госкорпорации «Росатом» защищенных с использованием шифровальных (криптографических) средств информационных и телекоммуникационных системы

Заявление
на осуществление контроля (оценки) уровня доверия и контроля приведения в соответствие требованиям Госкорпорации «Росатом» защищенных с использованием шифровальных (криптографических) средств информационных и телекоммуникационных систем

«___» _____ 201__ г.

_____

_____

_____
наименование организации, включая организационно-правовую форму

в лице _____
должность

_____
фамилия, имя, отчество

действующего на основании _____

просит Орган криптографической защиты АО «Гринатом» осуществить контроль (оценку) уровня доверия и контроль приведения в соответствие требованиям Госкорпорации «Росатом» защищенных с использованием шифровальных (криптографических) средств информационных и телекоммуникационных систем, указанных в таблице ниже.

Копии заключаемых/заключенных договоров на Систему(ы) (доп. соглашений) и приложения к ним и аттестата соответствия требованиям безопасности объекта информатизации, где обрабатывается конфиденциальная информация прилагаются.

№ п/п	Наименование информационной/ телекоммуникационной системы, защищенной с использованием шифровальных (криптографических) средств	Учетный номер АРМ/сервера, на котором установлена/ планируется установка Системы	Адрес месторасположения АРМ/сервера, на котором установлена/ планируется установка Системы	Наименования и версии СКЗИ, антивирусных средств, СЗИ от НСД и др. средств защиты информации, установленных на АРМ/сервере, на котором установлена/ планируется установка Системы

Уполномоченное должностное лицо

_____ _____ _____
(должность) (подпись) (ФИО)

м.п.

Приложение №5. Шаблон Заключения ОКЗ

УТВЕРЖДАЮ

<указывается должность>

_____/_____
(подпись) (Ф.И.О)

«___»_____ 20__ г.

ЗАКЛЮЧЕНИЕ
по результатам оценки уровня доверия к
<указывается наименование Системы>

г. Москва

1. ВВОДНАЯ ЧАСТЬ

1.1. Основание для выдачи заключения

Указываются реквизиты договора, на основании которого проводятся работы.

1.2. Наименование защищенной с использованием шифровальных (криптографических) средств информационной системы

Указывается наименование Системы.

1.3. Вопросы для исследования

– Обеспечение доверия к технологии, реализующей инфраструктуру ключевой системы;
– Обеспечение доверия к средствам криптографической защиты, входящим в состав системы обработки данных;
– Обеспечение доверия к средствам обработки и отображения данных;
– Обеспечение доверия к участникам процессов обработки данных;
– Риски информационной безопасности, связанные с договорными отношениями с *<указывается наименование Системы>*.

2. ИССЛЕДОВАТЕЛЬСКАЯ ЧАСТЬ

Оценка уровня доверия к Системе проводится в соответствии с Едиными отраслевыми методическими указаниями по дистанционному банковскому обслуживанию в Госкорпорации «Росатом» и ее организациях, утвержденных Приказом от 22.10.2015 №1/1009-П (далее – ЕОМУ).

2.1. Методы исследования

- Анализ представленной в Орган криптографической защиты АО «Гринатом» документации на Систему;
- Анализ договора на использование Системы на предмет наличия рисков информационной безопасности.

3. В ПРОЦЕССЕ ИССЛЕДОВАНИЯ УСТАНОВЛЕНО

Для проведения исследования письмом *<указать реквизиты письма с запросом информации к Владельцу Системы>* была запрошена информация в *<указать наименование Владельца Системы>*. В ответ был получен ответ *<указать реквизиты ответа Владельца Системы>*.

3.1.Описание Системы

В данном разделе указывается описание Системы.

3.2. Схема сетевого взаимодействия

В данном разделе указывается схема сетевого взаимодействия Системы.

3.3. Классификация информации в Системе

Указываются заключения ПДТК о наличии или отсутствии в Системе конфиденциальной информации.

3.4. Инфраструктура ключевой системы

Указывается используемая ключевая система, программно-аппаратный комплекс удостоверяющего центра, дополнительные службы удостоверяющего центра, аккредитация удостоверяющего центра и другая информация в соответствии с методикой определения доверия к криптографическим сервисам, утв. Приказом от 22.10.2015 №1/1009-П (далее – Методика).

3.4.1. Жизненный цикл ключей пользователей Системы

Указывается жизненный цикл ключей пользователей Системы (процессы создания, передачи/получения, эксплуатации, хранения, замены и уничтожения), типы ключевых носителей и другая информация в соответствии с Методикой.

3.5. Жизненный цикл СКЗИ, использующихся в Системе

Указывается жизненный цикл СКЗИ, использующихся в Системе (процессы передачи/получения, эксплуатации, хранения, замены и уничтожения) и другая информация в соответствии с Методикой.

3.6. Механизм обеспечения конфиденциальности и целостности информации в Системе

Указывается механизм обеспечения конфиденциальности и целостности информации в Системе (используемые СКЗИ, протоколы) и другая информация в соответствии с Методикой.

3.7. Выполнение требований по безопасности информации на стороне Владельца Системы и на стороне организации-обладателя конфиденциальной информации

Указываются реквизиты документов, подтверждающих выполнение требований по безопасности информации на стороне Владельца Системы и на стороне организации-обладателя конфиденциальной информации.

3.8. Риски информационной безопасности, связанные с договорными отношениями с Владельцем Системы

Указываются реквизиты договора или ссылка на проект договора между Владельцем Системы и организацией-обладателем конфиденциальной информации и риски, связанные с договорными отношениями, согласно ЕОМУ.

4. ОЦЕНКА СООТВЕТСТВИЯ

4.1. Результаты исследования технологии, реализующей инфраструктуру ключевой системы

Критерий оценки	Наличие	Срок действия	Номер	Приложение №	Уровень доверия
Лицензия ФСБ России на соответствующие виды деятельности					
Документ, подтверждающий право использования на средство реализующее инфраструктуру ключевой системы (договор, лицензия и пр.)					
Документ, подтверждающий право использования на СКЗИ, использующееся в составе средства, реализующего инфраструктуру ключевой системы (договор, лицензия и пр.)					
Действующий сертификат соответствия ФСБ России на средство, реализующие инфраструктуру ключевой системы, сертифицированное в соответствии с системой сертификации РОСС RU.0001.030001 по классу не ниже КС2					
Действующий сертификат соответствия ФСБ России на средство криптографической защиты информации, использующееся для работы средства, реализующего инфраструктуру ключевой системы с классом защиты не ниже КС2					
В Банке используются сертифицированные ФСТЭК ключевые носители					
В Банке используются несертифицированные ФСТЭК ключевые носители					
Клиент использует сертифицированные ФСТЭК ключевые носители					

Клиент использует несертифицированные ФСТЭК ключевые носители					
Журнал поэкземплярного учета Банка с отметками об учете средств, реализующих инфраструктуру ключевой системы					
Документы, регламентирующие жизненный цикл ключевой системы					
Свидетельство об аккредитации					
Документ о выполнении Стандарта Банка России (Обеспечение информационной безопасности организаций банковской системы Российской Федерации)					
Наличие дополнительных служб удостоверяющего центра (службы онлайновой проверки статусов сертификатов и службы штампов времени)					
Поддержка формата усовершенствованной подписи					

4.2. Результаты исследований средств криптографической защиты, входящих в состав системы обработки данных

Критерий оценки	Наличие	Срок действия	Номер	Приложение №	Уровень доверия
Используются сертифицированные средства криптографической защиты информации					
Документ, подтверждающий право передачи СКЗИ, использующееся в работе Системы (договор, лицензия и пр.)					
Сертификаты соответствия ФСБ России на средства криптографической защиты информации с актуальным сроком действия (эксплуатирующиеся на рабочих местах пользователей Системы)					
Журнал поэкземплярного учета Банка с отметками об учете передаваемых Клиенту СКЗИ, эксплуатационной и технической документации к ним					
Журнал поэкземплярного учета Клиента с отметками об учете полученных СКЗИ от Банка, эксплуатационной и технической документации к ним					
Класс защиты применяющихся на рабочих местах пользователей Системы шифровальных (криптографических) средств не менее КС1					
Класс защиты применяющихся на рабочих местах пользователей Системы шифровальных					

(криптографических) средств не менее КС2					

4.3. Результаты исследований СФК, средств обработки и отображения данных

Критерий оценки	Наличие	Срок действия	Номер	Приложение №	Уровень доверия
Лицензия на программное обеспечение Системы					
Заключение Органа криптографической защиты о возможности эксплуатации СКЗИ на стороне Банка					
Заключение Органа криптографической защиты о возможности эксплуатации СКЗИ на стороне Клиента					
Копия формуляра на СКЗИ, полученного Банком от производителя, с отметкой об учётном номере дистрибутива СКЗИ и подтверждение получения из доверенного источника (акт приема-передачи и пр.)					
Копия формуляра на СКЗИ, полученного Клиентом от Банка, с отметкой об учётном номере дистрибутива СКЗИ и подтверждение получения из доверенного источника (акт приема-передачи и пр.)					
Заключение о корректности встраивания СКЗИ в Систему					
Документация на систему ДБО (техническое описание или техническая записка, инструкция пользователя, инструкция администратора безопасности)					
Документ, фиксирующий (подтверждающий) версию программного обеспечения Системы и регламент обновления Системы					
Аттестат соответствия ФСТЭК на Систему, АРМ, сеть, или сегмент сети, где обрабатывается конфиденциальная информация или средство построения доверенной среды на стороне Банка					
Аттестат соответствия ФСТЭК на Систему, АРМ, сеть, или сегмент сети, где обрабатывается конфиденциальная информация или средство построения доверенной среды на стороне Клиента					
Установлено сертифицированное антивирусное ПО на АРМ (сервере), где функционирует средство реализующие инфраструктуру ключевой системы					
Установлено сертифицированное антивирусное ПО на АРМ					

пользователей Системы на стороне Банка					
Установлено сертифицированное антивирусное ПО на АРМ пользователей Системы на стороне Клиента					
Установлено сертифицированное средство защиты от несанкционированного доступа (далее - СЗИ от НСД) на АРМ (сервере), где функционирует средство реализующие инфраструктуру ключевой системы					
Установлено сертифицированное СЗИ от НСД на АРМ пользователей Системы на стороне Банка					
Установлено сертифицированное СЗИ от НСД на АРМ пользователей Системы на стороне Клиента					

4.4. Результаты исследований участников процессов обработки данных

Критерий оценки	Наличие	Срок действия	Номер	Приложение №	Уровень доверия
Документ, подтверждающий допуск пользователей Банка к работе с СКЗИ в Системе					
Документ, подтверждающий допуск пользователей Клиента к работе с СКЗИ в Системе					
Документ, подтверждающий прохождение обучения пользователями Системы на стороне Банка					
Документ, подтверждающий прохождение обучения пользователями Системы на стороне Клиента					
Локальные нормативные акты, определяющие права и роли работников Банка в Системе (подписантов, администраторов безопасности)					
Локальные нормативные акты, определяющие права и роли работников Клиента в Системе (подписантов, администраторов безопасности)					
Контроль администраторами безопасности условий использования СКЗИ на стороне Банка					

5. ВЫВОДЫ И РЕКОМЕНДАЦИИ

5.1. Выводы

На момент составления Заключения по полученной от *<указывается наименование Владельца Системы>* информации Система обеспечивает *<указывается выявленный уровень* доверия> уровень доверия. Согласно ЕОМУ в организациях Госкорпорации «Росатом» допустим уровень доверия не ниже среднего.

5.2. Рекомендации

Для приведения Системы к среднему уровню доверия Орган криптографической защиты АО «Гринатом» рекомендует *<указывается наименование Владельца Системы>* провести следующие работы в краткосрочной перспективе:

<указывается перечень мероприятий по приведению системы к среднему уровню доверия>.

Для приведения Системы к высокому уровню доверия Орган криптографической защиты АО «Гринатом» рекомендует *<указывается наименование Владельца Системы>* провести следующие работы в среднесрочной перспективе:

<указывается перечень мероприятий по приведению системы к высокому уровню доверия>.

Для приведения Системы к среднему уровню доверия Орган криптографической защиты АО «Гринатом» рекомендует *<указывается наименование организации-обладателя конфиденциальной информации>* провести следующие работы в краткосрочной перспективе:

<указывается перечень мероприятий по приведению системы к высокому уровню доверия>.

Для приведения Системы к высокому уровню доверия ОКЗ АО «Гринатом» рекомендует *<указывается наименование организации-обладателя конфиденциальной информации>* провести следующие работы в среднесрочной перспективе:

<указывается перечень мероприятий по приведению системы к высокому уровню доверия>.

Указываются рекомендации по изменению формулировок договора между Владельцем Системы и организацией-обладателем конфиденциальной информации для снижения рисков информационной безопасности, связанные с договорными отношениями, согласно ЕОМУ.

6. НОРМАТИВНАЯ И СПРАВОЧНАЯ ДОКУМЕНТАЦИЯ

Перечень нормативно-справочной документации и приложений.

Заключение составил:

<указывается должность>

_____/_____
(подпись) (Ф.И.О)

Ознакомлен:

<указывается должность>

_____/_____
(подпись) (Ф.И.О)

Исп: ФИО
Тел:

Приложение №6. Шаблон отчета о проведенных работах

УТВЕРЖДАЮ

<указывается должность>

_____/_____
(подпись) (Ф.И.О)

«___»_____ 20__ г.

Отчет о мероприятиях по приведению
<указывается наименование системы>
в соответствие с требованиями Единых отраслевых методических указаний по дистанционному банковскому обслуживанию в Госкорпорации «Росатом» и ее организациях

Период проведения обследования:
<указываются даты периода>

2018 г.

1. ВВОДНАЯ ЧАСТЬ

1.1. Основание для выполнения работ

Указываются реквизиты договора, на основании которого проводятся работы.

1.2. Наименование защищенной с использованием шифровальных (криптографических) средств информационной

Указывается наименование Системы.

1.3. Вопросы для исследования

Изменение уровня доверия к Системе за отчетный период.

2. Изменение статуса Системы за отчетный период

2.1. Уровень доверия к Системе на начало отчетного периода

По результатам выполнения работ по оценке уровня доверия к Системе было выдано *<указываются реквизиты выданного Заключения по результатам оценки уровня доверия Системе>* (далее - Заключение).

В соответствии с Заключением Система обеспечивает *<указывается уровень доверия согласно ранее выданному Заключению>* уровень доверия. Согласно Приказа Госкорпорации «Росатом» от 22.10.2015 № 1/1009-П «Об утверждении Единых отраслевых методических указаний по дистанционному банковскому обслуживанию в Госкорпорации «Росатом» и ее организациях» в организациях Госкорпорации «Росатом» допускается эксплуатация информационных систем с уровнем доверия не ниже среднего.

2.2. Замечания по Системе и перечень проведенных мероприятий

<Указывается перечень проведенных мероприятий в рамках приведения системы в соответствие с требованиями ЕОМУ>.

№ п/п	Недостатки, указанные в Заключении по результатам оценки уровня доверия к Системе	Рекомендации по устранению выявленных недостатков	Ответственный	Срок	Уровень доверия на начало периода	Уровень доверия на конец периода	Отметка о выполнении (выполнено/не выполнено)	Статус
Недостатки, выявленные на стороне *<указывается наименование Владельца Системы>*								
1								
2								
Недостатки, выявленные на стороне *<указывается наименование организации-обладателя конфиденциальной информации>*								
1								
2								

2.3. Уровень доверия к Системе на конец отчетного периода

На конец отчетного периода уровень доверия к Системе *<указывается изменился/не изменился>*. Уровень доверия соответствует *<указывается уровень доверия на конец отчетного периода>*.

Заключение составил:

<указывается должность>

_____/_____
(подпись) (Ф.И.О)

Ознакомлен:

<указывается должность>

_____/_____
(подпись) (Ф.И.О)

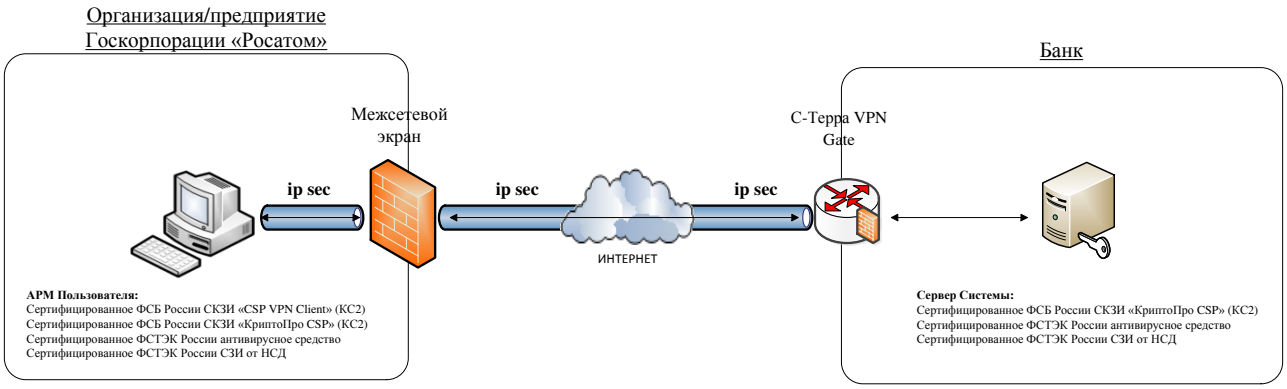
Исп: ФИО
Тел:

Приложение №7. Типовые схемы подключения

1. Обеспечение конфиденциальности[1], доступности[2] и целостности[3] информации

1.1. Средства криптографической защиты информации (вариант №1)

Физическая схема подключения автоматизированного рабочего места пользователя предприятия/организации Госкорпорации «Росатом» (далее - АРМ Пользователя) к серверу системы дистанционного банковского обслуживания (далее – Система):



АРМ Пользователя:

Для шифрования канала связи между АРМ Пользователя и сервером Банка на АРМ Пользователя устанавливаются сертифицированные ФСБ России средства криптографической защиты информации (далее – СКЗИ) «С-Терра CSP VPN Client» и СКЗИ «КриптоПро CSP» с классом защищенности не ниже КС2.

Сервер Банка:

На стороне Банка устанавливается сертифицированный ФСБ России ПАК «С-Терра VPN Gate» и СКЗИ «КриптоПро CSP» с классом защищенности не ниже КС2.

1.2. Средства криптографической защиты информации (вариант №2)

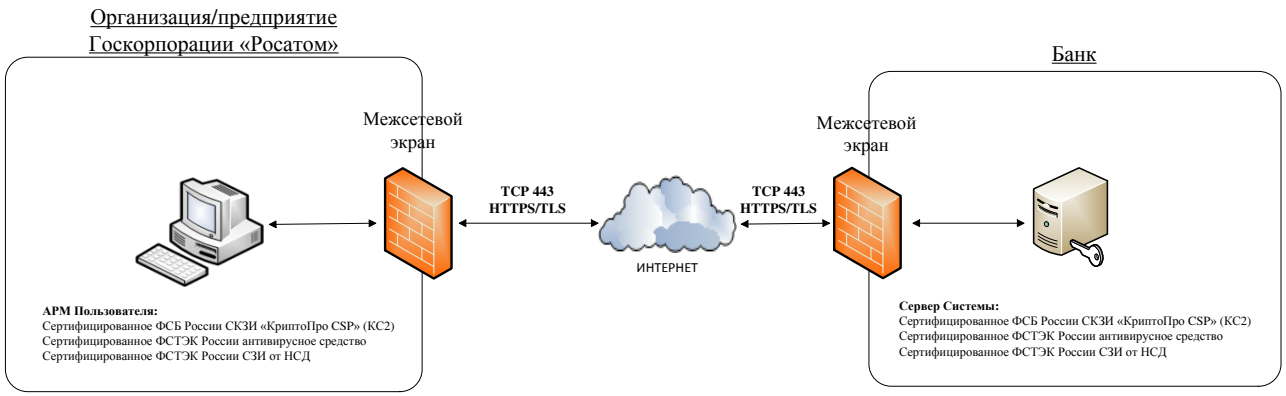
Физическая схема подключения АРМ Пользователя к серверу Системы:

---

[1] Конфиденциальность информации - состояние защищенности информации, характеризуемое способностью автоматизированной системы обеспечивать сохранение в тайне информации от субъектов, не имеющих полномочий на ознакомление с ней.

[2] Доступность информации - состояние информации, характеризуемое способностью автоматизированной системы обеспечивать беспрепятственный доступ к информации субъектов, имеющих на это полномочия.

[3] Целостность информации - состояние защищенности информации, характеризуемое способностью автоматизированной системы обеспечивать сохранность и неизменность конфиденциальной информации при попытках несанкционированных или случайных воздействий на нее в процессе обработки или хранения.



АРМ Пользователя:

Для шифрования канала связи между АРМ Пользователя и сервером Банка на АРМ Пользователя устанавливается сертифицированное ФСБ России СКЗИ «КриптоПро CSP» с классом защищенности не ниже КС2.

Сервер Банка:

На стороне Банка устанавливается сертифицированное ФСБ России СКЗИ «КриптоПро CSP» с классом защищенности не ниже КС2.

2. Защита информации от несанкционированного доступа

Для обеспечения защиты информации от несанкционированного доступа на стороне Банка и на стороне предприятия/организации Госкорпорации «Росатом» должны выполняться требования следующих документов:

– инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну, утв. Приказом ФАПСИ от 13 июня 2001г. №152;

– единых отраслевых методических указаниях по дистанционному банковскому обслуживанию в Госкорпорации «Росатом» и ее организациях, утв. Приказом Госкорпорации «Росатом» от 22.10.2015 №1/1009-П;

На стороне предприятия/организации Госкорпорации «Росатом» также должны выполняться:

– отраслевые требования по информационной безопасности Госкорпорации «Росатом» от 13.07.2012;

– отраслевые требованиями по информационной безопасности, утв. Приказом от 23.09.2014 №1/910-П-дсп.

Программно-технические средства защиты, которые должны быть установлены на АРМ Пользователей и на сервере Системы:

– Сертифицированное ФСТЭК России антивирусное программное обеспечение.

Эксплуатация АРМ Пользователей без установленного антивирусного программного обеспечения или его отключение не допускается. Антивирусная проверка поступающей на АРМ Пользователей информации осуществляется в автоматическом режиме;

– Сертифицированное ФСТЭК России средство защиты информации от несанкционированного доступа.

В качестве средств защиты от несанкционированного доступа необходимо использовать средства, указанные в эксплуатационной и технической документации на СКЗИ «КриптоПро CSP», С-Терра CSP VPN Client или ПАК «С-Терра VPN Gate» (Аппаратно-программный модуль доверенной загрузки универсальный М-526Б «КРИПТОН-ЗАМОК/У» или ПАК защиты от НСД «Соболь» RU.40308570.501410.001)

3. Выполнение требований по безопасности информации

АРМ Пользователей и сервер Системы должны соответствовать требованиям по безопасности информации и иметь соответствующие аттестаты соответствия.

Органом криптографической защиты должна быть проведена проверка выполнения требований Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну, утв. Приказом ФАПСИ от 13 июня 2001г. №152 на АРМ Пользователя Системы и на сервере Банка, где установлены СКЗИ. Подтверждением возможности эксплуатации СКЗИ в Системе является Заключение Органа криптографической защиты о возможности эксплуатации СКЗИ.