Приложение № 21 к Договору присоединения № 22/2143-Д от 6 июля 2012 г.

УТВЕРЖДАЮ
Директор по информационным технологиям
АО «Гринатом»

_____ В.В. Золотов
М.П.

П О Р Я Д О К
предоставления услуг Технологического удостоверяющего центра

Москва
2024

Содержание

1. Назначение и область применения

Настоящий Порядок предоставления услуг Технологического удостоверяющего центра (далее – Порядок) разработан для установления последовательности действий по процессам:

- Предоставление сертификатов для аутентификации устройств в ЛВС, стандарт IEEE 802.1x.
- Предоставление SSL/TLS-сертификатов для web-приложений информационных систем, web сайтов, серверов, домен-контроллеров.
- Предоставление сертификатов на отчуждаемом носителе (смарт-карте) для пользовательской и(или) специальной учетной записи для обеспечения «строгой» аутентификации и «высокого» уровня доверия в соответствии с ГОСТ Р 58833-2020.
- Обеспечение жизнедеятельности сертификатов;

2. Термины, сокращения и аббревиатуры

2.1. Термины и определения

Термин	Определение
Активное сетевое оборудование	В соответствии с ГОСТ Р 51513-99, активное сетевое оборудование — это оборудование, содержащее электронные схемы, получающее питание от электрической сети или других источников и выполняющее функции усиления, преобразования сигналов и иные.
Владелец сертификата	Владельцем сертификата является: • Для SSL-сертификата руководитель рабочей группы, отвечающий за поддержку службы, приложения, сервиса; • Работник для которого был выпущен и выдан сертификат на отчуждаемом носителе;
Заявитель	работник подавший заявление на выпуск сертификата. Штатный работник рабочей группы отвечающий за поддержку службы, приложения, активного сетевого оборудования для которого запрашивается сертификат. Для проектной деятельности заявителем является РП.
Менеджер услуги	Лицо ответственное за предоставление услуги CLB.34
Оператор ТУЦ	Работник отдела криптографической защиты информации, который отвечает за обработку СЗ в СУ ИТ, выпуск, отзыв сертификата, а так же передачу сертификата заявителю.
Отчуждаемы носитель	Активный ключевой носитель (портативное устройство) в котором реализованы криптографические методы подписания документов электронной подписью и строгой двухфакторной аутентификации. Отчуждаемые носители могут быть различных форм-факторов, иметь как контактный, так и бесконтактный интерфейс. Могут содержать дополнительный идентификатор RFID для СКУД..
Приложение	Программное обеспечение, выполняющее функции, необходимые для предоставления ИТ-услуги. Каждое Приложение может быть частью более чем одной ИТ-услуги. Приложение может иметь одну или более серверных или клиентских частей.
Руководитель рабочей группы СУ ИТ (ответственный за поддержку приложения)	Руководитель рабочей группы, координирует работу подчиненной ему группы, отвечает за работоспособность приложения, предоставляющего услугу.
Цифровой сертификат (технологический сертификат)	представляет собой электронный документ, содержащий открытую часть ключевой пары, информацию о владельце сертификата, центре сертификации выпустившим его и др. дополнительную информацию.
Услуга	Способ предоставления ценности заказчикам через содействие им в получении конечных результатов, которых Заказчики хотят достичь без владения специфическими затратами и рисками.
Центры сертификации (Certificate authority- CA)	Центры сертификации (ЦС) образуют ТУЦ, развернуты на базе Windows Server. Состав: RosatomRootCA, RosatomIntCA01, RosatomIntCA02, InteratomCA01

2.2. Сокращения, используемые в целях данного документа, и расшифровки.

Сокращение	Расшифровка
ДИТ	Департамент информационных технологий
КСПД	Корпоративная сеть передачи данных

ЛВС	Локальная вычислительная сеть.
СЗ	Стандартный запрос в СУ ИТ
СУ ИТ	Система управления ИТ (Информационные Технологии)
СКУД	Система контроля и управления доступом
ТР	Техническое решение
ТУЦ	Технологический удостоверяющий центр
ЭЦП	Электронная цифровая подпись

2.3. Аббревиатуры и расшифровки.

Аббревиатура	Расшифровка
Стандарт 802.1x	Стандарт IEEE 802.1x определяет протокол контроля доступа и аутентификации, который ограничивает права неавторизованных компьютеров и устройств, подключенных к коммутатору. Сервер аутентификации проверяет каждый компьютер (устройство) перед тем, как тот сможет воспользоваться сервисами, которые предоставляет ему коммутатор.
Autoenrollment	Поддерживает автоматическое распространение сертификатов для компьютеров и пользователей на основе шаблонов версии 2 и 3.
CRL	— это «список цифровых сертификатов, которые были отозваны выдавшим их центром сертификации (CA) до истечения запланированного срока действия и которым больше не следует доверять»
CDP и AIA	В расширении «CRL Distribution Points (CDP)» хранятся ссылки на CRL издавшего конкретный сертификат CA; В расширении «Authority Information Access (AIA)» хранятся ссылки на сертификат CA, издавшего конкретный сертификат.
RFID	Radio Frequency IDentification. Радиочастотная идентификация использует электромагнитные поля для автоматической идентификации и отслеживания меток, прикрепленных к объектам. RFID-система состоит из крошечного радиопередатчика, радиоприемника и передатчика. При срабатывании электромагнитного опросного импульса от ближайшего устройства считывания RFID метка передает цифровые данные, обратно считывателю.
ssca.rosatom.ru	Web-ресурс на котором размещаются CRL ТУЦ, сертификаты корневого и издающего Центра сертификации.
SSL/TLS-сертификат	это электронный документ, содержащий открытый ключ, информацию о владельце ключа, области применения ключа. Позволяет системам проверять клиента и впоследствии устанавливать зашифрованное сетевое соединение с другой системой с использованием протокола Secure Sockets Layer/Transport Layer Security (SSL/TLS).

3. Описание процесса

3.1 Цель процесса

Предоставление технологических сертификатов:

- для аутентификации устройств в ЛВС, стандарт IEEE 802.1x.
- для web-приложений информационных систем, web сайтов, серверов, домен-контроллеров (SSL/TLS-сертификат).
- на отчуждаемом носителе (смарт-карте) для пользовательской и(или) специальной учетной записи для обеспечения «строгой» аутентификации и «высокого» уровня доверия в соответствии с ГОСТ Р 58833-2020.

3.2 Задачи процесса

- Обработка запроса на выпуск сертификата;
- Создание сертификата, передача заявителю;
- Проверка срока действия выпущенных сертификатов;
- Оповещение заявителей об истечении срока действия сертификата (через специальные группы рассылки);
- Обеспечение жизнедеятельности сертификата;
- Отзыв сертификата, т.е. аннулирование ранее выданного сертификата, имеющего активный (не просроченный) срок действия;

3.3 Участники группы процессов и их роли

Уполномоченное лицо	• Принимает решение о необходимости получения услуг ТУЦ; • Согласовывает документы, необходимые для получения услуг ТУЦ; • Принимает решение о прекращении получения услуг ТУЦ;
Заявитель	• Подготавливает и согласовывает документы на получение услуг ТУЦ; • Получает сертификат;
Владелец сертификата	• Отвечает за целевое использование сертификата; • Устанавливает сертификат в целевую систему, приложение; • Отслеживает срок действия сертификата и своевременно принимает решение о перевыпуске или аннулировании сертификата; • Уничтожает сертификат при выведение его из действия либо после окончания срока действия;
Менеджер услуги	• Обрабатывает обращения; • Принимает решения на создание и сокращение подписки; • Ведет базу актуальных сертификатов; • Обеспечивает работоспособность ТУЦ в комплексе и предоставление сервисов для корректной работы сертификатов;
Оператор ТУЦ	• Работает с обращениями; • Выпускает сертификаты и передает заявителю; • Отзывает сертификаты;

3.4 Описание процесса «Предоставление услуг ТУЦ»

3.4.1 Подпроцесс «Обработка обращения»

Менеджер услуги получает обращение одним из следующих способов:
электронное письмо на п/я 1111@greenatom.ru;
звонок в центр поддержки пользователей АО «Гринатом»;
СЗ из каталога услуг в СУ ИТ;
заявление в бумажной форме;
заявление направленное через ЕОСДО;

- Определяет наличие Подписки у организации;
- Определяет необходимость выдачи нового носителя

В случае выдачи нового носителя, стоимость оплачивается единоразово по составляющей CLB.34 «Услуги ТУЦ, Сертификат выпущенный оператором на отчуждаемом носителе», в ином случае применяется составляющая CLB.34 «Услуги ТУЦ, поддержка ранее выпущенного действующего сертификата на смарт-карте»;

- Формализует обращение в зависимости от следующих условий:

В случае отсутствия Подписки у организации и обращение не на создание Подписки, то процесс завершается;

В случае если Подписки нет, а обращение на создание подписки, то исходящая информация поступает в подпроцесс «Создание подписки»;

В случае если Подписка есть, а обращение на сокращение подписки, то исходящая информация поступает в подпроцесс «Вывод из эксплуатации», в случае если обращение не связано с сокращением подписки, а с необходимостью выпустить сертификат, то исходящая информация поступает в подпроцесс «Обеспечение технологическими сертификатами», если сертификат выпускать не надо, то в «Обеспечение функционирования».

3.4.2 Подпроцесс «Создание подписки»

Входящая информация поступает из подпроцесса «Обработка обращений»
Заявитель:

- Формирует заявку на создание подписку;

Организации отрасли подают заявления согласно п.3.4.1 (Приложение № 1 или № 3-5). Работники АО «Гринатом» делают СЗ из каталога услуг в СУ ИТ «7.10. Запрос выпуска сертификата», 10.04.01 «Получение сертификата спец. УЗ на смарт-карте», Задание на изменение.

Уполномоченное лицо:

- Подписывает (согласовывает) заявку;

Для заявок, созданных в СУ ИТ, уполномоченным лицом является непосредственный руководитель или руководитель рабочей группы для которой запрашивается подписка.

Менеджер услуги:

- получает заявку, оценивает соответствие параметров запрашиваемого сертификата возможностям ТУЦ;

В случае если возможности ТУЦ позволяют создать такой сертификат и его использование не противоречит ЕОМУ по информационной безопасности ГК «Росатом», то исходящая информация поступает в подпроцесс «Обеспечение технологическими сертификатами».

3.4.3 Подпроцесс «Обеспечение технологическими сертификатами»

Входящая информация поступает из подпроцессов «Создание подписки» или «Обработка обращения»

В случае если сертификат выпускает оператор ТУЦ, то он берет заявку в работу. Проверяет корректность предоставленных данных, если данные корректные выпускает сертификат и передает заявителю установленным порядком, если данные не корректны отклоняет заявку и уведомляет об этом заявителя.

Сертификат созданный оператором ТУЦ не записанный не отчуждаемый носитель, передается свободным поручением в ЕОСДО или путём записи на учтённый флэш накопитель.

Владелец сертификата:

- Устанавливает сертификат в целевое устройство, службу, приложение;

В случае если заявителю разрешено самостоятельно запрашивать сертификат, то он через консоль управления сертификатами формирует запрос на его создание, в ответ на запрос получает сертификат и устанавливает его.

Если устройства, подключенные к сети, поддерживают автоматическую подачу заявок на сертификаты (Autoenrollment), то ЦС автоматически обрабатывает такие запросы, генерирует сертификат и передает его на устройство.

Исходящая информация поступает в подпроцесс «Обеспечение функционирования»

3.4.4 Подпроцесс «Обеспечение функционирования»

Входящая информация поступает из подпроцессов «Обработка обращения» и/или «Обеспечение технологическими сертификатами».

Процесс обеспечения функционирования ТУЦ лежит на отделе криптографической защиты, при этом обеспечивается:

- Предоставление доступа к CDP и AIA на web-ресурсе ssca.rosatom.ru, необходим для корректной работы сертификата; (если web-ресурс ssca.rosatom.ru для устройства, службы, приложения в котором установлен сертификат не доступен, то согласованием открытия СВ обеспечивает владелец сертификата)
- Механизм проверки срока действия сертификата и уведомление владельца сертификата об окончании срока его действия;

Проверка срока действия сертификата происходит с периодичностью 1 раз в 7дней.

В случае если срок действия сертификата истекает, то владельцу сертификата по эл.почте выдаётся уведомление об окончании его срока действия.

В случае если сервис (оборудование) находятся в эксплуатации, то владелец сертификата инициирует перевыпуск сертификата, исходящая информация поступает в подпроцесс «Обеспечение технологическим сертификатом»;

В случае если сервис (оборудование) выведено из эксплуатации, владелец сертификата инициирует задачу по аннулированию сертификата, исходящая информация поступает в подпроцесс «Вывод из эксплуатации»;

Для активного сетевого оборудования, поддерживающего режим Autoenrollment, проверка срока действия сертификата происходит на самом оборудовании без участия ТУЦ.

В случае если до окончания срока действия сертификата остается менее 20% времени от общего срока действия, то оборудование формирует автоматический запрос на создание нового сертификата. Далее исходящая информация поступает в подпроцесс «Обеспечение технологическими сертификатами».

3.4.5 Подпроцесс «Вывод из эксплуатации»

Входящая информация поступает из подпроцесса «Обработка обращения», связанного с сокращением подписки.

Владелец сертификата:

- формирует заявку на сокращение подписки

Организации отрасли подают заявления согласно п.3.4.1. Работники АО «Гринатом» делают СЗ из каталога услуг в СУ ИТ «07.11. Запрос отзыва (аннулирования) сертификата от ТУЦ»

Уполномоченное лицо:

- согласовывает заявку на сокращение подписки.

В случае если уполномоченное лицо не согласовывает сокращение подписки исходящая информация поступает в подпроцесс «Обеспечение функционирования»;

Оператор ТУЦ:

- аннулирует сертификат;

Сведения об аннулированном сертификате заносит в реестр выданных сертификатов, на этом подпроцесс заканчивается.

4. Порядок внесения изменений

Внесение изменений (дополнений) в Порядок, а также в Приложения к нему, производится посредством утверждения новой редакции Порядка. Новая версия Порядка вступает в силу через 10 (десять) дней после публикации на сайте КУЦ.

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

5. Контроль и ответственность

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

Заявитель несёт ответственность за:

- сохранность переданного ему сертификата, выпущенный сертификат предназначен для инсталляции в системы, указанные в первичном обращении, передача сертификата третьим лицам.

Владелец сертификата несёт ответственность:

- За сохранность сертификата, за передачу сертификата лицам, имеющим легитимные основания работать с ним;
- за отслеживание срока действия сертификата, при уведомлении об ожидаемом истечения срока действия сертификата, обязан инициировать процесс выпуска нового сертификата.
- своевременно инициировать процесс отзыва сертификата, если приложение для которого выпускался сертификат выведено из промышленной эксплуатации.

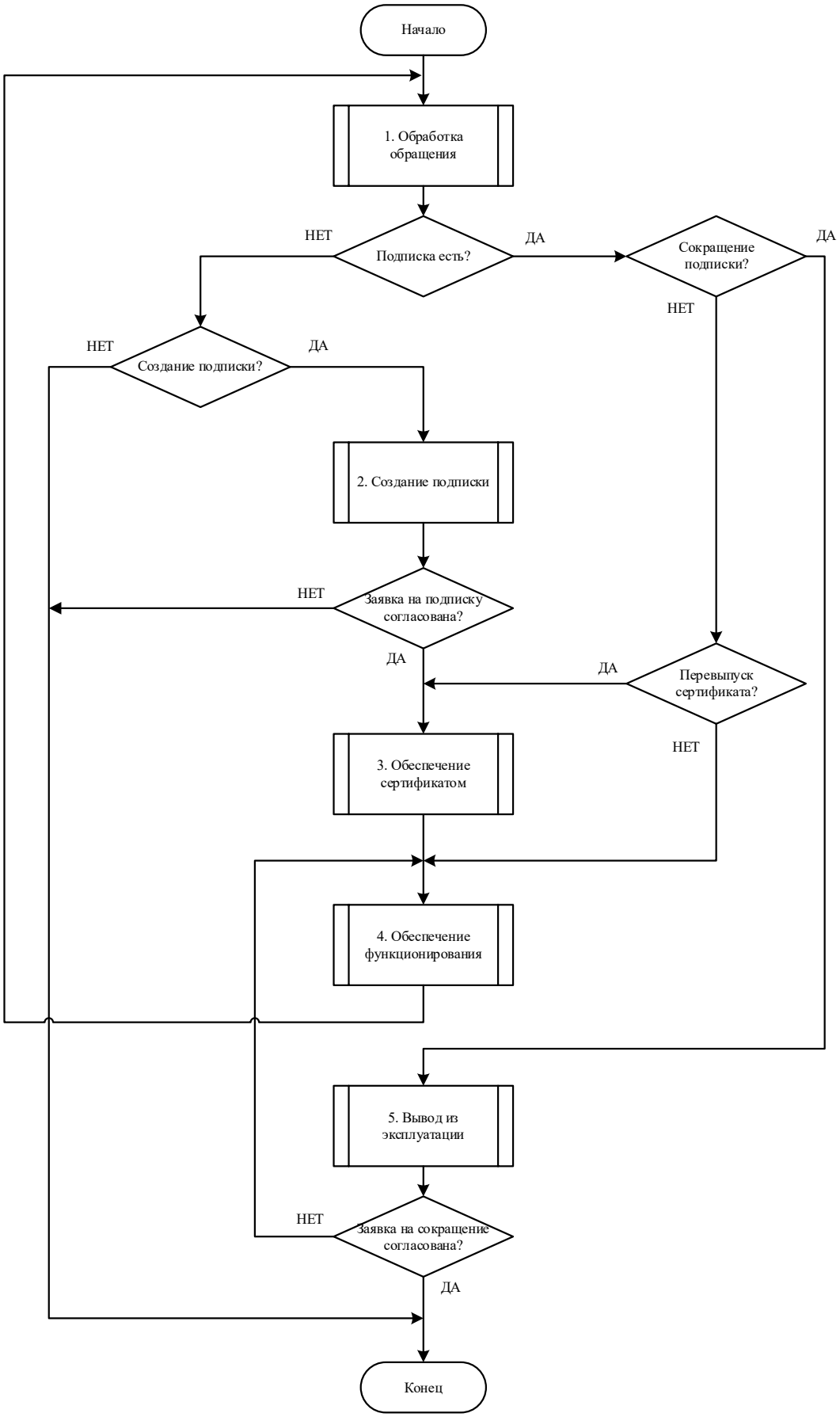
Оператор ТУЦ несёт ответственность:

- за выдачу сертификата;
- за передачу выпущенного сертификата только владельцу сервиса (приложения) для которого он был запрошен. Передача сертификата третьим лицам не допускается. Передача сертификата заявителю, открытым каналом связи не допускается;
- за корректное выполнение работ в которых осуществляется отзыв сертификата;
- за ведение реестра выданных сертификатов, достоверность информации в нем.
- за качество предоставления услуги.

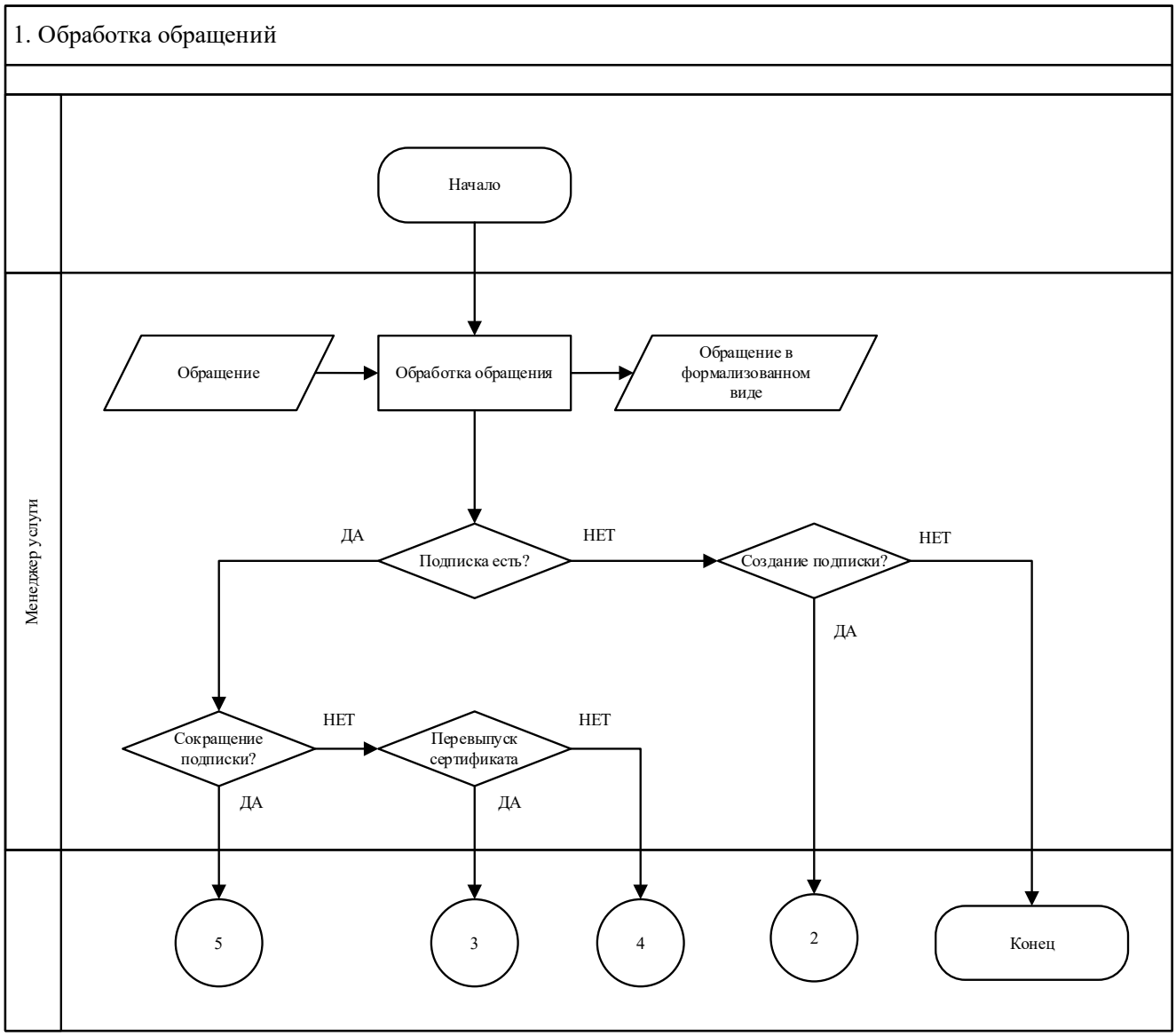
Менеджер услуги ТУЦ несёт ответственность:

- за работоспособность ТУЦ и вспомогательных сервисов, обеспечивающих работу ТУЦ в комплексе.
- за корректную работу механизма проверки срока действия активных сертификатов;
- за качество предоставления услуги.

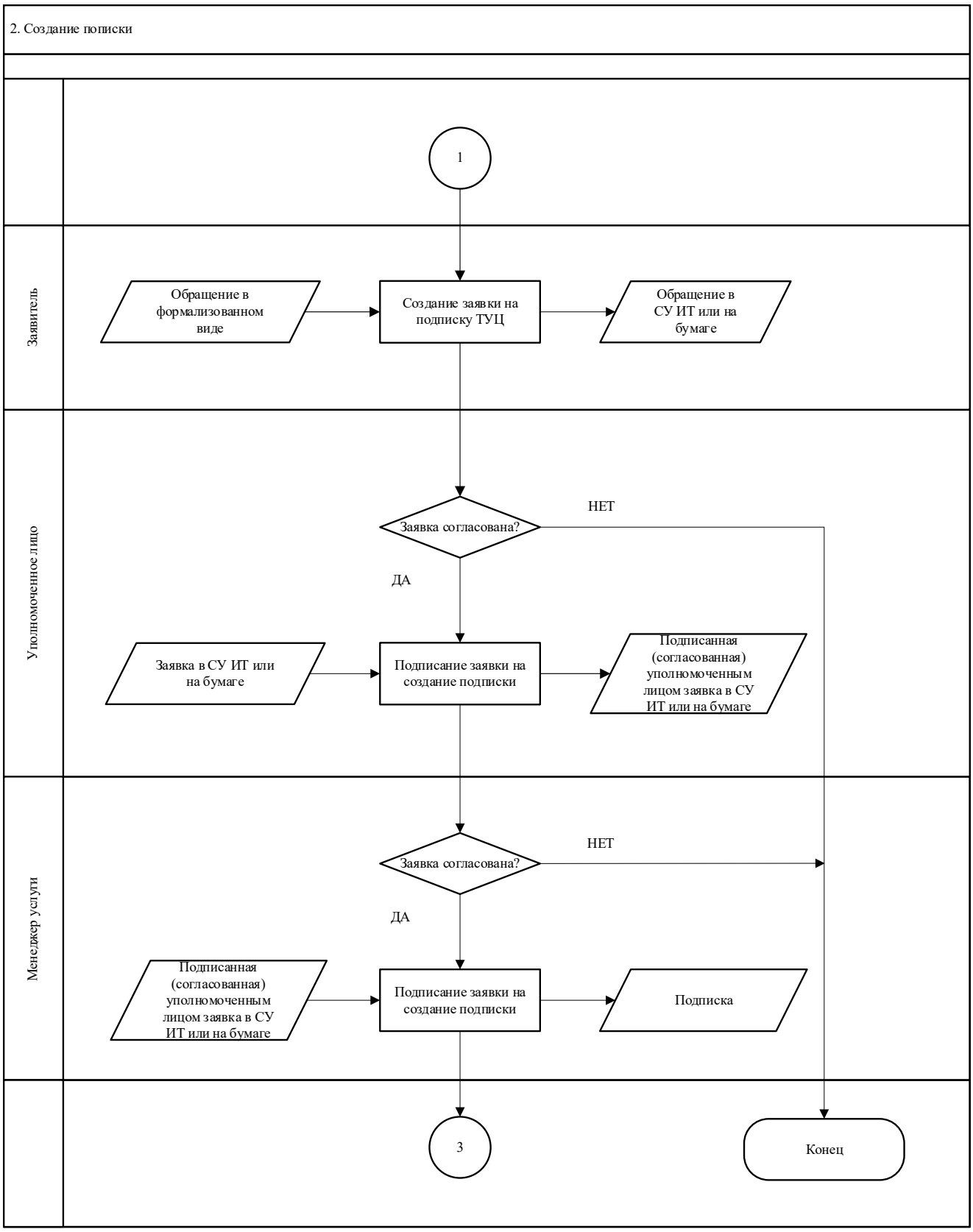
6. Схема процесса «Предоставление услуг ТУЦ»



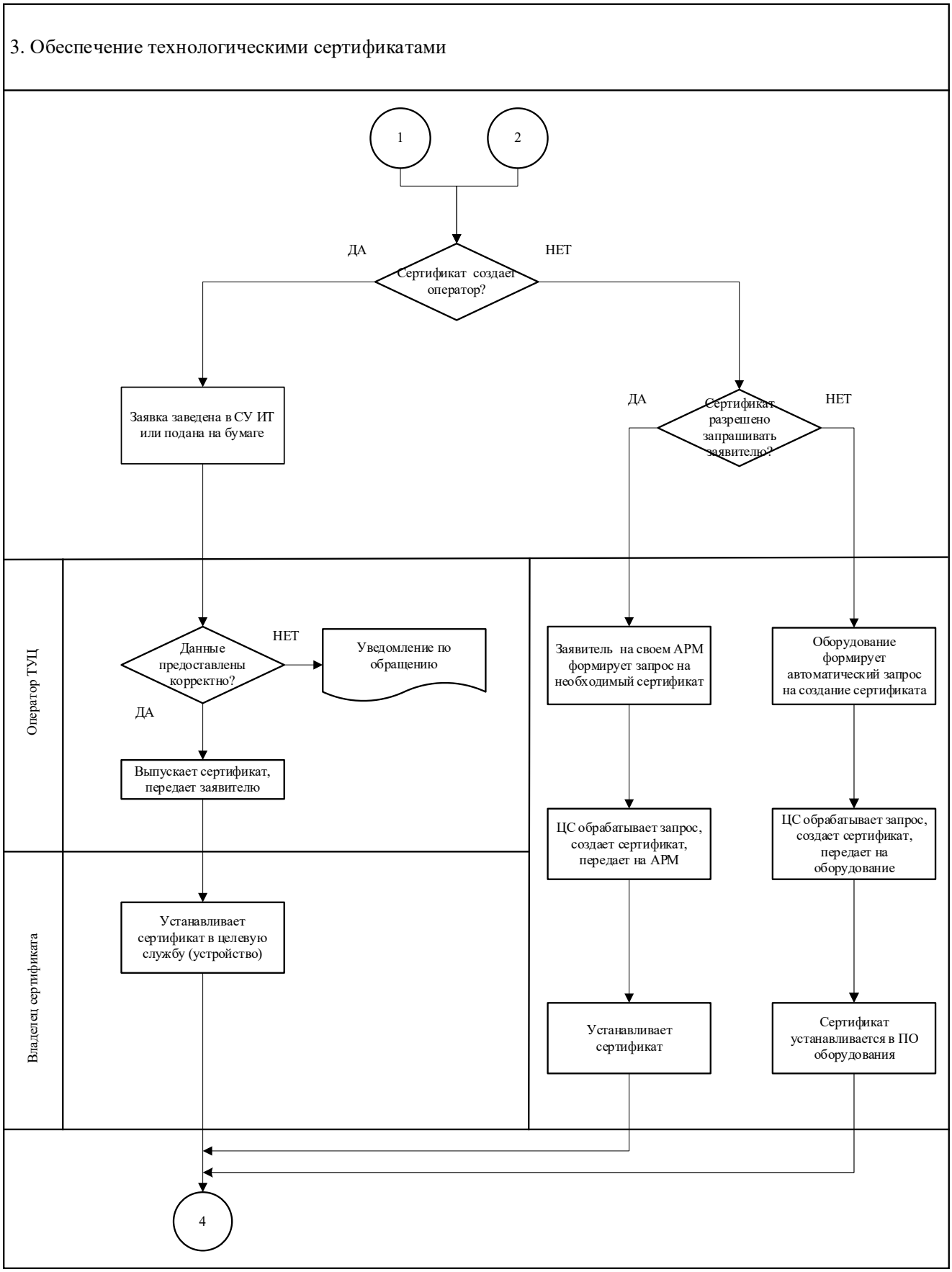
6.1 Схема подпроцесса «Обработка обращения»



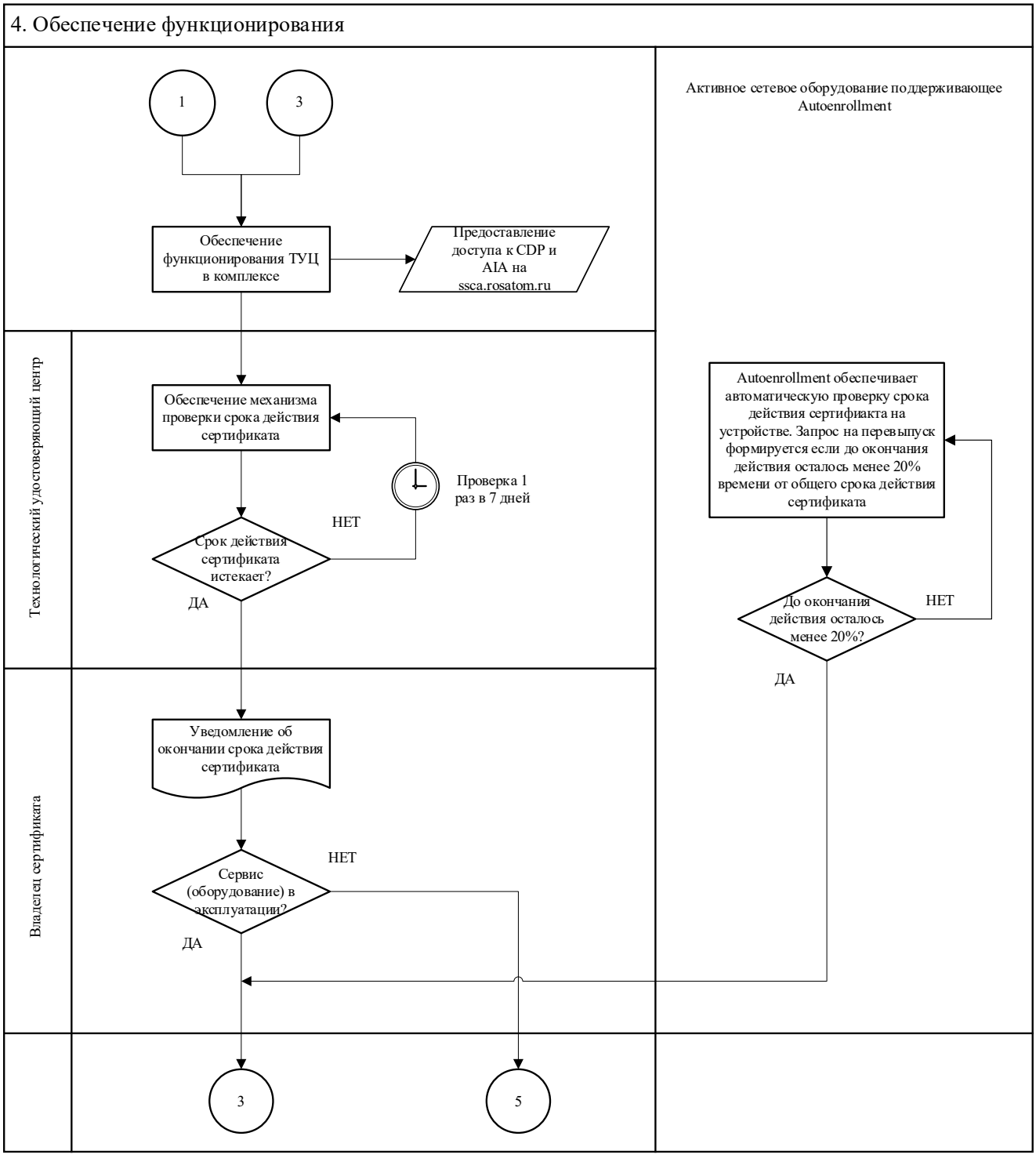
6.2 Схема подпроцесса «Создание подписки»



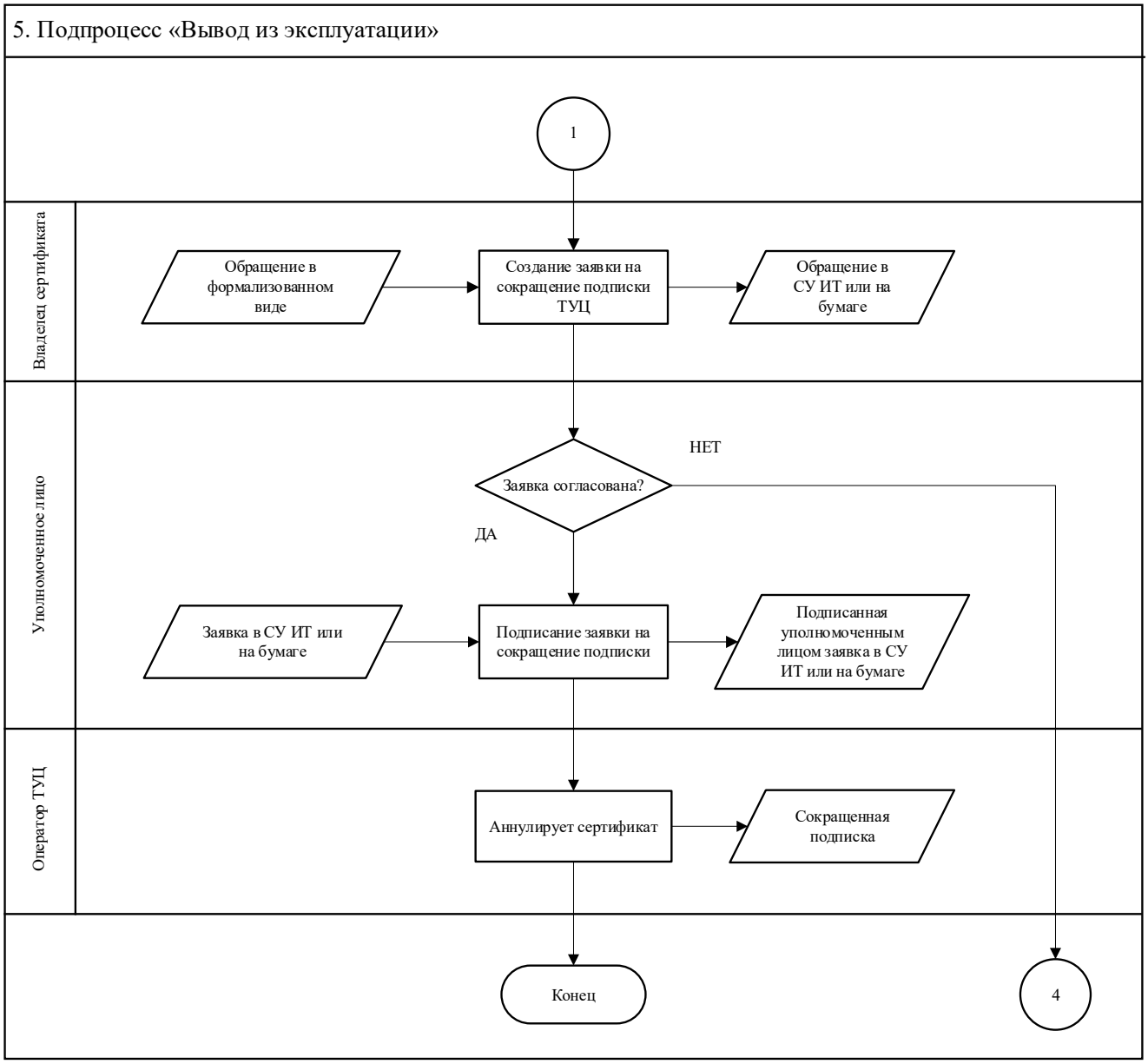
6.3 Схема подпроцесса «Обеспечение технологическими сертификатами»



6.4 Схема подпроцесса «Обеспечение функционирования»



6.5 Схема подпроцесса «Вывод из эксплуатации»



7. Перечень приложений

Приложение № 1: Заявление на обеспечение технологическими сертификатами для аутентификации в сети по стандарту 802.1x на основе сертификатов

Заявление на обеспечение технологическими сертификатами для аутентификации в сети по стандарту 802.1x на основе сертификатов

«___» _____ 202__г

_____
наименование организации, включая организационно-правовую форму

в лице _____
должность

_____
фамилия, имя, отчество

действующего на основании _____

просит:

Обеспечить технологическими сертификатами следующее оборудование:

	Тип оборудования и ОС	Количество	Поддержка Autoenrollment
1.			
2.			
3.			
4.			
5.			
6.			
7.			

Ответственные лица от заявителя:

_____
Должность, ФИО

_____ _____ _____
Рабочий телефон Доб. № Мобильный телефон e-mail:

Уполномоченное должностное лицо

_____ _____ _____
Должность М.П. Подпись И.О. Фамилия

Приложение № 2: Заявление на аннулирование сертификата

Заявление на аннулирование сертификата

«___» _____ 202__г

_____

наименование организации, включая организационно-правовую форму

в лице _____

должность

_____

фамилия, имя, отчество

действующего на основании _____

просит аннулировать сертификат(ы):

№ п/п	Номер сертификата	Причина аннулирования
1.		
2.		
3.		
4.		
5.		
6.		
7.		
8.		
9.		
10.		
11.		
12.		
13.		
14.		

Уполномоченное должностное лицо

_____ _____ _____

Должность М.П. Подпись И.О. Фамилия

Отметки ТУЦ

Отметка Оператора ТУЦ. _____/_____/
Данные указанные в заявлении, проверены.
Сведения об аннулировании сертификата занесены в реестр ТУЦ «____» _____202___г.

Приложение № 3: Заявление на выпуск сертификата технологическим удостоверяющем центром.

Заявление на выпуск сертификата
технологическим удостоверяющем центром АО «Гринатом»

«___» _____ 202__г

_____
наименование организации, включая организационно-правовую форму

в лице _____
должность

_____
фамилия, имя, отчество

действующего на основании _____
просит выпустить сертификат со следующими параметрами:

Поля	Значения
Имя сертификата (CN Common Name)	
Дополнительные имена (Subject Alternative Name) - должны быть включены все имена, которые могут быть использованы, DNS имя.	
Шаблон сертификата (CertificateTemplate) – варианты: Web Server, ТАРМ 802.1x, Custom	

Дополнительная информация:

Приложение (сервис) – для функционирования которого, запрошен сертификат	
Email владельца сертификата (руководитель рабочей группы) – указывается владельцем сервисной или проектной группы рассылки. Определяется менеджером услуги.	

Ответственные лица от заявителя:

1. _____
Должность, ФИО

_____ _____ _____
Рабочий телефон Доб. № Мобильный телефон e-mail:

2. _____
Должность, ФИО

_____ _____ _____
Рабочий телефон Доб. № Мобильный телефон e-mail:

Уполномоченное должностное лицо

_____ _____ _____
Должность М.П. Подпись И.О. Фамилия

Приложение № 4: Заявление на выпуск сертификата для специальной УЗ на отчуждаемом носителе (смарт-карте).

Заявление на выпуск сертификата для специальной УЗ на отчуждаемом носителе (смарт-карте) технологическим удостоверяющем центром АО «Гринатом»

«___» _____ 202__г

_____

наименование организации, включая организационно-правовую форму

в лице _____

должность

_____

фамилия, имя, отчество

действующего на основании _____

просит выпустить сертификат на смарт-карте со следующими параметрами:

Поля	Значения
ФИО пользователя	
Email адрес основной УЗ пользователя	
Имя основной УЗ пользователя	
Имя специализированной УЗ пользователя (пример: gren-a-name)	

Предоставить смарт-карту и сертификат (отметить галочкой):

В Технологическом удостоверяющем центре по адресу: г. Москва, 1-й Нагатинский пр-д, д.10, стр.1	☐
Службой специальной связи по адресу* (указать адрес, ФИО администратора безопасности и телефон): *-кроме Москвы и Московской области	☐

Владелец сертификата _____ _____

Подпись И.О. Фамилия

Уполномоченное должностное лицо

_____ _____ _____

Должность М.П. Подпись И.О. Фамилия

Приложение № 5: Заявление на выпуск сертификата для пользовательской УЗ на отчуждаемом носителе (смарт-карте).

Заявление
на выпуск сертификата для пользовательской УЗ на отчуждаемом носителе (смарт-карте) технологическим удостоверяющем центром АО «Гринатом»

«___» _____ 202__г

_____
наименование организации, включая организационно-правовую форму

в лице _____
должность

_____
фамилия, имя, отчество

действующего на основании _____
просит выпустить сертификат на смарт-карте со следующими параметрами:

№ п/п	ФИО пользователя	Имя учетной записи
1.		
2.		
3.		
4.		
5.		
6.		
7.		
8.		
9.		
10.		

Предоставить смарт-карту и сертификат (отметить галочкой):

В Технологическом удостоверяющем центре по адресу: г. Москва, 1-й Нагатинский пр-д, д.10, стр.1	☐
Службой специальной связи по адресу* (указать адрес, ФИО администратора безопасности и телефон): *-кроме г.Москвы и Московской области	☐

Ответственное лицо от заявителя (АБ):

_____
Должность, ФИО

_____ _____
Рабочий телефон Доб. № e-mail:

Уполномоченное должностное лицо

_____ _____ _____ _____
Должность М.П. Подпись И.О. Фамилия

Приложение № 6: Реестр выданных сертификатов ТУЦ

Имя сертификата (Issued to)	Серийный номер (Serial number)	Дата начала действия (Valid form)	Окончание срока действия (Valid to)	Шаблон сертификата	Номер задачи в СУ ИТ в раках которого выпускался сертификат	Владелец	Рабочая группа в СУ ИТ	Email рассылки (для уведомления)	Имена серверов (на которые установлен сертификат)	Приложение (сервис)	Статус